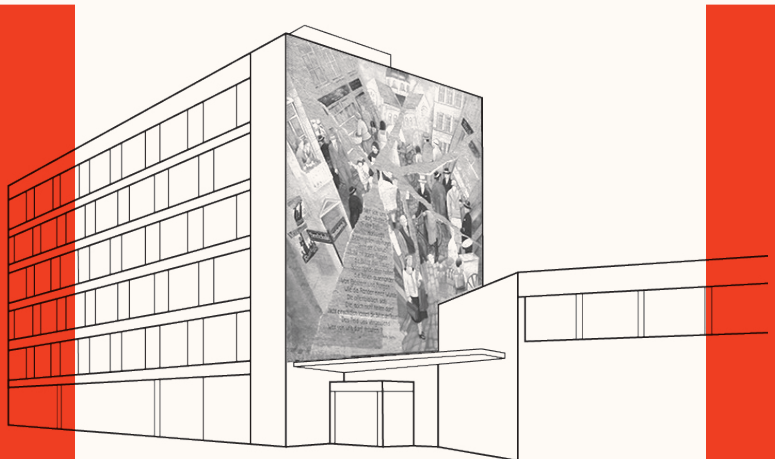

Marita Körner

Die Datenschutzgrundverordnung der Europäischen Union: Struktur und Ordnungsprinzipien

Rechtswissenschaftliche
Beiträge der
Hamburger Sozialökonomie

Heft 12

Marita Körner

Die Datenschutzgrundverordnung der Europäischen Union: Struktur und Ordnungsprinzipien

Rechtswissenschaftliche
Beiträge der
Hamburger Sozialökonomie

Heft 12

Prof. Dr. Marita Körner
Professorin für Deutsches und Internationales Arbeits- und Sozialrecht und Rechtsvergleichung am Fachbereich Sozialökonomie der Fakultät für Wirtschafts- und Sozialwissenschaften an der Universität Hamburg; Zweitmitglied der Fakultät für Rechtswissenschaft der Universität Hamburg.

Impressum

Kai-Oliver Knops, Marita Körner, Karsten Nowrot (Hrsg.)
Rechtswissenschaftliche Beiträge der Hamburger Sozialökonomie

Heft 12, März 2017

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikations in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet unter http://dnb.dnb.de abrufbar.

ISSN 2366-0260 (print)
ISSN 2365-4112 (online)

Reihengestaltung: Ina Kwon
Produktion: UHH Druckerei, Hamburg
Schutzgebühr Euro 5

Die Hefte der Schriftenreihe „Rechtswissenschaftliche Beiträge der Hamburger Sozialökonomie“ finden sich zum Download auf der Website des Fachgebiets Rechtswissenschaft am Fachbereich Sozialökonomie unter der Adresse:

https://www.wiso.uni-hamburg.de/fachbereich-sozoek/professuren/koerner/fiwa/publikationsreihe.html

Fachgebiet Rechtswissenschaft
Fachbereich Sozialökonomie
Fakultät für Wirtschafts- und Sozialwissenschaften
Universität Hamburg
Von-Melle-Park 9
20146 Hamburg

Tel.: 040 / 42838 - 3521
Fax: 040 / 42838 - 8129
E-Mail: Beate.Hartmann@wiso.uni-hamburg.de

Inhalt

A. Einleitung*

Der Datenschutz ist ein junges Rechtsgebiet – das erste Datenschutzgesetz der Welt, das des Bundeslandes Hessen, datiert von 1970.[1] Das Thema erlebte eine erste Hochzeit in den 1980er Jahren, insbesondere durch das Volkszählungsurteil des Bundesverfassungsgerichts (BVerfG), das aus den Art. 2 Abs. 1 und Art. 1 Abs. 1 GG ein Recht auf informationelle Selbstbestimmung ablas. Danach muss jeder Einzelne grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen können.[2]

In dieser Epoche der Datenverarbeitung, vor 40 Jahren also, erfolgte Datenverarbeitung in Rechenzentren mit Großrechnern. Personenbezogene Daten sammelte vor allem der Staat, demgegenüber es den Einzelnen durch Datenverarbeitungsvorgaben zu schützen galt. Aus dieser Anfangszeit stammt der Grundsatz des Verbots mit Erlaubnisvorbehalt, wonach die Erhebung, Speicherung und Verarbeitung personenbezogener Daten gesetzlich oder durch Einwilligung des Betroffenen gerechtfertigt sein muss. Nach einem Datenschutzjahrzehnt in den 1980er Jahren geriet das Thema aus dem Blick der Öffentlichkeit, also der Betroffenen. Entsprechend zäh verlief seine Weiterentwicklung. Die Innovationszyklen der Informationstechnologie nahmen dagegen immer mehr Fahrt auf – seit 1993 ist das Internet allgemein zugänglich, aber der Datenschutz blieb bei seinen alten Strukturen.

Eine zweite Welle des allgemeinen Interesses am Datenschutz wurde zum einen durch Skandale im Zusammenhang mit Beschäftigtendaten[3] in den Jahren 2007/ 2008 ausgelöst. Zum anderen klärten die Enthüllungen des ehemaligen US-amerikanischen Geheimdienstmitarbeiters Edward Snowdon im Jahr 2013 über das zwar von manchen befürchtete, aber von vielen nicht für möglich gehaltene Ausmaß der weltweiten Sammlung, Speicherung, Neuzusammenfügung und kommerziellen, aber auch staatlichen und geheimdienstlichen Nutzung von personenbezogenen Daten von Abermillionen Menschen auf. Das war möglich geworden, da sich auch die Speichertechnik und Auswertungsverfahren rasant weiterentwickelt haben. Gefahren für die Privatsphäre drohen heute aber nicht mehr nur vom datensammelnden kontrollafinen Staat, sondern vor allem von Unternehmen, die personenbezogene Daten als einen der lukrativsten Märkte des 21. Jahrhunderts entdeckt haben. Big Data ist hier nur ein Stichwort. Dabei geht es darum, durch die Auswertung einst für ganze andere Zusammenhänge gesammelter großer Datenmengen Trends zu erkennen, zukünftiges Verhalten zu berechnen oder Investitionsentscheidungen zu steuern.

Vor diesem Hintergrund hat die Europäische Union (EU) im Jahr 2012 einen Verordnungsentwurf zum Datenschutz vorgelegt, der eine janusköpfige Antwort auf die skizzierte Entwicklung liefern sollte: den Weg frei machen, um das wirtschaftliche Potential der Digitalisierung zu erschließen, ohne den Schutz der Betroffenen völlig über Bord zu werfen. Entsprechend hatte die 2012 zuständige Kommissarin Vivian Reding bei der Vorstellung des Kommissionsentwurfs der Datenschutzgrundverordnung (DS-GVO) die wirtschaftlichen Chancen für den digitalen Binnenmarkt durch personenbezogene Daten hervorgehoben und betont, dass die europäische Bevölkerung in ihrer Funktion als Verbraucher und Verbraucherinnen ohne ausreichenden Datenschutz zu verhalten auf die digitalen Angebote reagiert.

* Es handelt sich um einen leicht modifizierten Auszug aus einer umfangreichen Untersuchung für das HSI (HSI-Schriftenreihe Bd. 18, 2016).

1 GVBl. I 1970, 625.

2 BVerfG 65, 1.

3 *Körner*, AuR 2010, 416, 417.

Auch die Digitalisierung der Arbeitswelt ist so weit fortgeschritten, dass man in Anlehnung an die industrielle Revolution des 19. Jahrhunderts von einer digitalen Revolution sprechen kann, die die Arten von Arbeit, die Strukturen, in denen Arbeit erbracht wird, und nahezu alle bisherigen Beschäftigungsformen grundlegend verändern wird.[4] Diese Entwicklung hat rechtlich betrachtet mindestens zwei Seiten, zum einen die arbeitsrechtliche, bei der es um sozialen Schutz der (abhängig) beschäftigten Menschen geht, der sich bei fluiden, virtuellen Formen der Arbeitserbringung immer weniger mit den seit Jahrzehnten entwickelten und bewährten arbeitsrechtlichen Instrumenten gewährleisten lässt. Zum anderen geht es um die datenschutzrechtliche Seite dieser Entwicklung, die dazu führt bzw. in vielen Bereichen schon dazu geführt hat, dass ein privater, abgeschirmter, vor Blicken von außen geschützter Raum für Individuen kaum noch existiert. Ob und inwieweit die DS-GVO hier eine wirksame „Firewall" errichten kann, steht nicht im Mittelpunkt der folgenden Untersuchung, darf aber schon deshalb bezweifelt werden, weil das europäische Recht zum einen bereits keinen Zugriff auf das globale Phänomen Digitalisierung aller Lebensbereiche hat. Zum anderen greift DS-GVO trotz gegenteiliger Beteuerung ihrer Macher im Wesentlichen auf die alten Instrumente zurück, die seit Jahren als unzureichend kritisiert werden, und nur punktuell vermeintlich Neues einführt, das aber bei näherer Betrachtung in internationalem Zusammenhang oft nur schwer oder gar nicht kontrollierbar sein wird, etwa ein Recht auf Vergessenwerden.

Lange war unbestritten, dass wirkungsvoller Datenschutz bereichsspezifischer Datenschutz sein muss,[5] weil nur Regelungen, die die konkreten Verarbeitungsformen berücksichtigen, deren besondere Gefahren eindämmen können. Das hat sich auch in § 1 Abs. 3 BDSG niedergeschlagen, wonach das BDSG hinter bereichsspezifischen Regelungen zurücktreten muss. Angesichts der Digitalisierung aller Lebensbereiche würde ein vorwiegend bereichsspezifischer Ansatz allerdings zu einem unübersehbaren Regelungsdickicht und damit in der Praxis zu weniger Schutz führen.[6] Insofern ist der generell-abstrakte Ansatz der DS-GVO vernünftig. Der Verordnungsgeber sieht aber selbst, dass es Lebensbereiche gibt, wo die generellen Regelungen nicht ausreichen und öffnet daher die Grundverordnung, trotz des obersten Zieles der Rechtsvereinheitlichung, für nationale „spezifischere" Regelungen.

B. Genese der DS-GVO seit 2012

Am 4.5.2016 wurde die Europäische Datenschutzgrundverordnung (DS-GVO) im Amtsblatt der EU veröffentlicht[7] und trat am 25.5.2016 in Kraft, nachdem der Rat am 8.4.2016 und das Europäische Parlament am 14.4.2016 die endgültige Fassung förmlich angenommen hatten. Nach einer zweijährigen Übergangszeit wird sie gemäß ihres Art. 99 Abs. 2 am 25.5.2018 für staatliche Stellen und Unternehmen anwendbar – wie schon die Datenschutzrichtlinie von

4 Vgl. zur Digitalisierung der Arbeitswelt: Bundesministerium für Arbeit und Soziales (Hrsg.), Grünbuch – Arbeiten 4.0, Berlin 2015 sowie vor allem zu den Auswirkungen auf die Arbeitszeit das Gutachten von *Rüdiger Krause* zum 71. DJT 2016: Digitalisierung der Arbeitswelt – Herausforderungen und Regelungsbedarf, Verhandlungen des 71. Deutschen Juristentags, Band I: Gutachten/Teil B, Essen 2016; *Giesen/Junker/Rieble* (Hrsg.), Industrie 4.0 als Herausforderung des Arbeitsrechts, ZAAR Schriftenreihe, Band 39, München 2016; *Däubler*, Digitalisierung und Arbeitsrecht, SR Sonderheft, Juli 2016.

5 Vgl. etwa *Simitis*, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 2014, 8. Auflg., Einleitung Rn. 20.

6 Zum Problem der eventuellen Überregulierung durch bereichsspezifischen Datenschutz: *Kingreen/ Kühling*, JZ 2015, 213.

7 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

1995 gilt die DS-GVO gleichermaßen für den öffentlichen wie den privaten Bereich. Auch wenn die DS-GVO als EU-Verordnung gemäß Art. 288 AEUV unmittelbar anwendbar ist, gibt es erheblichen nationalen Anpassungsbedarf. Abgesehen davon, dass die DS-GVO mit ihren 99 Artikeln und 173 Erwägungsgründen viel umfangreicher ist als das BDSG und daher allein schon die Anpassung der Datenverarbeitungsprozesse an die neuen Regelungen eine Herausforderung darstellt, hat der europäische Gesetzgeber nun doch, trotz des ursprünglichen Hauptziels der Verordnung, den Datenschutz europaweit zu harmonisieren, zahlreiche Regelungsgegenstände dem nationalen Gesetzgeber zur Konkretisierung oder gar, wie beim Beschäftigtendatenschutz in Art. 88 DS-GVO, umfassend den Einzelstaaten zur Ausgestaltung überlassen.[8]

Dabei hat der vierjährige europäische Gesetzgebungsprozess mehrere Stadien durchlaufen, die nicht nur von historischem Interesse sind, sondern wichtig bei der Auslegung der schließlich verabschiedeten Version, die ebenso wie die erste von 2012 unzählige unbestimmte Rechtsbegriffe und Generalklauseln enthält. Bereits im Januar 2012 hatte die Europäische Kommission einen Reformvorschlag für das europäische Datenschutzrecht vorgelegt,[9] nachdem Datenschutzrecht auf europäischer Ebene umfassend erstmals 1995 in einer Richtlinie thematisiert worden war[10] und nach rund zwei Jahrzehnten rasanter Digitalisierung nahezu aller Lebenszusammenhänge eine europäische Datenschutzantwort auf die Entwicklung der Informationstechnologie überfällig war. Diese Fassung löste große Kontroversen mit ca. 4.000 Änderungsvorschlägen aus.[11] U.a. wurde kritisiert, dass sich die Kommission selbst in 26 Fällen im Wege sogenannter delegierter Rechtsakte Konkretisierungsbefugnisse für in der Verordnung nur vage formulierte Regelungen eingeräumt hatte. Das Europäische Parlament legte im März 2014 eine modifizierte Fassung vor, in die zahlreiche der Änderungsvorschläge eingegangen sind.[12] U.a. wurde die Anzahl der Kommissionsermächtigungen zu delegierten Rechtsakten auf zehn reduziert. Der Rat machte seine Verhandlungsposition zur DS-GVO und damit die Sichtweise der Mitgliedstaaten am 11.6.2015 deutlich.[13] Damit reagierte er auf den Kommissionsentwurf von 2012, nicht aber auf die Fassung des Europäischen Parlaments. Delegierte Rechtsakte zugunsten der Kommission sind in der Ratsfassung nahezu vollständig verschwunden.

Schließlich einigten sich Kommission, Parlament und Rat im Dezember 2015 im informellen Trilog auf die Version, die dann im April 2016 im Wesentlichen unverändert verabschiedet wurde. Allerdings wurde in der endgültigen Version z.T. noch einmal die Nummerierung der Artikel geändert, was die Nachverfolgung der Argumentationslinien partiell erschweren kann.

8 So auch *Kühling/Martini et al.,* Die Datenschutzgrundverordnung und das nationale Recht, 2016, S. 298.

9 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) vom 25.1.2012: KOM (2012) 11 endg.

10 Richtlinie des Europäischen Parlaments und des Rates 95/46/EG vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG Nr. L 281 S. 31 ff.

11 *Hornung,* ZD 2012, 104; *Schild/Tinnefeld*, DuD 2012, 312.

12 TA 2014/212/P7. Dazu *Roßnagel/Kroschwald*, ZD 2014, 495.

13 Rat der Europäischen Union, Dok. 9565/15. Dazu *Roßnagel/Nebel/Richter*, Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO, ZD 2015, 455.

C. Ziele und Hauptinhalte der DS-GVO

I. Bisheriger Datenschutz

1. Nationale Ebene

Das deutsche Datenschutzrecht ist stark ausdifferenziert und war nicht von vornherein verfassungsrechtlich verankert. Mehr als eine Dekade vor dem Volkszählungsurteil des BVerfG von 1983 basierte es auf den im Laufe der Zeit inhaltlich stark angenäherten Landesdatenschutzgesetzen und dem Bundesdatenschutzgesetz. Der in diesen Gesetzen geregelte allgemeine Datenschutz wurde im Laufe der Jahrzehnte durch eine große Zahl an bereichsspezifischen Regelungen im öffentlichen wie im privaten Bereich ergänzt, die gemäß § 1 Abs. 3 BDSG immer Vorrang vor den allgemeinen Bestimmungen haben. Zum bereichsspezifischen Datenschutz zählt etwa der Sozial- und Gesundheitsdatenschutz (insbesondere § 35 SGB I i.V.m. §§ 67 ff. SGB X) oder das Telemedien- sowie Telekommunikationsdatenschutzrecht (§§ 1 ff. TMG und §§ 91 ff. TKG), aber auch viele Einzelregelungen, wie etwa § 14 SigG, § 21g EnWG oder § 213 VVG.[14] Trotz des Vorrangs bereichsspezifischer Regelungen gibt es allerdings immer wieder Abgrenzungsprobleme.[15]

Erst 1983 erfolgte die verfassungsrechtliche Verankerung durch das im Volkszählungsurteil aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG abgeleitete Recht auf informationelle Selbstbestimmung als Abwehrrecht des Einzelnen gegen staatliche Eingriffe,[16] dem 2008 das kurz als IT-Grundrecht bezeichnete Recht auf die Vertraulichkeit informationstechnischer Systeme[17] zur Seite gestellt wurde. Seit gut 30 Jahren also ist Datenschutz in Deutschland auch ein verfassungsrechtliches Thema mit allen materiellrechtlichen wie prozessrechtlichen Implikationen – eine individuelle Verfassungsbeschwerde zum BVerfG gemäß § 90 BVerfGG ist im Prinzip möglich.

2. Europäische Ebene

Vor diesem Hintergrund wurde der europäische Datenschutz nicht selten eher als Schutz minderer Qualität angesehen. Ohnehin trat der EU-Gesetzgeber mit der Datenschutzrichtlinie von 1995[18] spät auf den Plan[19] und hatte zudem nur bedingt neue Ideen zu bieten. Im Großen und Ganzen basierte die Richtlinie auf dem deutschen Datenschutzrecht, enthielt aber auch den einen oder anderen Einzelpunkt, der zuvor national nicht realisierbar war und dann im Zuge der Umsetzung der Richtlinie ins BDSG aufgenommen wurde. Die Beteiligung des EuGH an der Fortentwicklung des Datenschutzes blieb marginal. Ein Übriges tat der Umstand, dass die meisten EU-Mitgliedstaaten die Datenschutzrichtlinie nicht angemessen umgesetzt hatten – im Jahr 2016 der Hauptgrund für eine Verordnung als Regelungsinstrument für den europäischen Datenschutz.

14 Weitere Beispiele bei *Gola/Schomerus*, BDSG-Kommentar, 2015, 12. Auflg., Einleitung Rn. 8.
15 Vgl. etwa für den Telemedienbereich *Keppeler*, MMR 2015, 779 f.
16 BVerfGE 65, 1 ff.; dazu *Grimm*, JZ 2013, 585 f.
17 BVerfGE 120, 274 ff.
18 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Abl. Nr. L 281 S. 31.
19 *Simitis*, Die EG-Datenschutzrichtlinie: eine überfällige Reformaufgabe, in: Herzog/Neumann (Hrsg.), Festschrift für Winfried Hassemer, 2010, S. 1235.

Erst seit der Charta der Grundrechte der EU (GR-Charta) aus dem Jahr 2000[20] zeichnet sich auch auf EU-Ebene eine Konstitutionalisierung des Datenschutzes ab. Zwar war die Grundrechte-Charta zunächst nur eine politische Erklärung und damit nicht rechtsverbindlich, was sich aber mit dem Vertrag von Lissabon durch Art. 6 Abs. 1 EUV seit dem 1.12.2009 änderte. Seitdem ist die Charta der Grundrechte und damit auch ihr Art. 8, der ein Grundrecht auf den Schutz personenbezogener Daten gewährleistet, rechtlich für den gesamten Geltungsbereich des Unionsrechts bindend. Jüngst hat der EuGH in drei wichtigen Entscheidungen deutlich gemacht, wie er das europäische Grundrecht auf Datenschutz zu konturieren gedenkt.[21] Aus prozessualer Sicht ist allerdings schon hier darauf hinzuweisen, dass je nachdem, ob man sich im harmonisierten – EU-Grundrechte – oder nicht harmonisierten Bereich – nationale Grundrechte – befindet, nur im letzteren Bereich noch die individuelle Verfassungsbeschwerde als Rechtsbehelf zur Verfügung steht, was auf Unionsebene nicht der Fall ist.[22]

3. EU-Grundrechte und nationale Grundrechte: ein ungeklärtes Verhältnis

Das Verhältnis zwischen Unionsrecht, insbesondere EU-Grundrechten und nationalem Verfassungsrecht ist komplex und gehört zu den umstrittensten Bereichen des Verfassungs- und Europarechts,[23] was damit zusammenhängt, dass die Frage weder im nationalen noch im EU-Recht geregelt ist und es daher allein auf die Rechtsprechung des EuGH und des BVerfG ankommt. Die war seit der Entscheidung des EuGH bereits aus dem Jahr 1964, wonach Unionsrecht wegen seiner besonderen Rechtsnatur Anwendungsvorrang vor nationalem Recht hat[24] und der rasch darauf getroffenen EuGH-Entscheidung, dass das auch für das Verfassungsrecht der Mitgliedstaaten gilt,[25] lebhaft. Das BVerfG erkennt den Anwendungsvorrang zwar prinzipiell an,[26] allerdings nur – und das betont das Gericht auch noch 2009 in seiner Entscheidung zum Lissabon-Vertrag – aufgrund des deutschen Zustimmungsgesetzes. Das heißt, dass das BVerfG den Vorrang des Unionsrechts nicht für absolut hält, sondern „nur kraft und im Rahmen der verfassungsrechtlichen Ermächtigung“.[27]

Für das Verhältnis zwischen deutschen Grundrechten und dem sekundären Unionsrecht gibt es seit der Solange II-Entscheidung aus dem Jahr 1986 nichts grundlegend Neues.[28] Hatte das BVerfG im Jahr 1974 noch entschieden, dass die Übertragung von Hoheitsrechten auf die EU unzulässig sei, wenn dadurch, z.B. durch den Erlass von Verordnungen, die Grundrechte des GG beeinträchtigt werden können (Solange I),[29] so ist das BVerfG eine Dekade später zu einer anderen Bewertung gekommen. Mittlerweile hielt es die Einhaltung der Grundrechte durch die Rechtsprechung des EuGH dadurch für gewährleistet, dass der EuGH grundrechtsgleiche allgemeine Rechtsgrundsätze aus den Verfassungstraditionen der Mitgliedstaaten abgeleitet hatte, mit der Folge, dass das BVerfG seitdem die Vereinbarkeit von EU-Recht mit dem GG nicht mehr prüft (Solange II). Eine Hintertür hatte sich das Gericht offen gelassen: Sollte der vom GG gewährte Grundrechtsschutz – im vorliegenden Zusammenhang das Recht auf informationelle Selbstbestimmung – auf EU-Ebene „generell“ nicht mehr gewährleistet

20 Charta der Grundrechte der Union, ABl. 2000 Nr. C 364/01.
21 Dazu näher unten C.VII.2.b). Zum europäischen Datenschutzgrundrecht in Art. 8 GR-Charta vgl. auch *Heuschmid/Lörcher*, NK-GA, Art. 8 GR-Charta.
22 *Heuschmid/*Lörcher, NK-GA, Art. 51 Rn. 9 ff.
23 *Polzin*, JuS 2012, 1, Fn 3 m.w.N.; dazu auch schon *Körner*, ZESAR 2013, 153, 155 ff.
24 EuGH, Urt. v. 15.7.1964 – 6/64, Slg. 1964, 1251, 1269 f. (Costa/E.N.E.L.).
25 EuGH, Urt. v. 17.12.1970 – 11/70, Slg. 1970, 1125 (Internationale Handelsgesellschaft).
26 BVerfGE 31, 145, 174.
27 BVerfGE 123, 267, 354; BVerfG, Urt. v. 21.6.2016 – 2 BvR 2728/13.
28 *Masing*, JZ 2015, 477, 480.
29 BVerfGE 37, 271, 279 f.

werden, käme wieder das GG für die Prüfung von EU-Sekundärrecht zum Zuge.[30] Neben diesem grundrechtlichen Kontrollanspruch hat sich das BVerfG im Maastricht-Urteil für das Handeln von Unionsorganen eine Ultra-vires-Kontrolle vorbehalten,[31] wonach im Einzelfall geprüft werden kann, ob Kompetenzgrenzen für den Erlass von EU-Rechtsakten offensichtlich verletzt wurden. Diese Linie wurde im Lissabon-Urteil bestätigt und durch den weiteren Vorbehalt einer Identitätskontrolle ergänzt.[32] Es geht dabei um die Identität des GG, die in Art. 79 Abs. 3 GG garantiert ist und nicht aufgegeben werden darf sowie um bestimmte, sich aus Art. 20 Abs. 1 und 2 sowie Art. 38 Abs. 1 S. 1 GG ergebende Bereiche, die zur Gewährleistung „demokratischer Selbstgestaltungsfähigkeit“[33] nicht auf die EU übertragen werden dürfen.[34]

Seitdem ist die europäische GR-Charta in Kraft getreten, die in Art. 8 sogar ein eigenes Datenschutzgrundrecht enthält, sodass von einer „generell“ nicht gewährleisteten Grundrechtssicherung auf EU-Ebene keine Rede sein kann. Es gilt gemäß Art. 51 Abs. 1 GR-Charta eine Art Arbeitsteilung: für vereinheitlichtes Unionsrecht, wie in der DS-GVO der harmonisierte Teil, gilt der EU-Grundrechtsschutz,[35] für das einzelstaatliche Recht die Grundrechte der jeweiligen Verfassung.[36] Hieraus ergebe sich allerdings, so der ehemalige Bundesverfassungsrichter *Masing*, ein „Grundrechtsüberdruck“.[37] Beim Datenschutz ist dieser durch die Konkurrenz zwischen dem ausdrücklichen Datenschutzgrundrecht in Art. 8 GR-Charta und der aus Art. 2 Abs. 1 GG abgeleiteten informationellen Selbstbestimmung besonders sichtbar und fällt eher zugunsten der EU-Grundrechte aus,[38] zumal der EuGH sich von der Abgrenzung der Grundrechtssphären in Art. 51 Abs. 1 GR-Charta kaum beeindrucken lässt und darauf abstellt, ob die vom Mitgliedstaat angewandte Rechtsnorm „in den Anwendungs- oder Geltungsbereich“ des Unionsrechts fällt.[39] Das war in der Rechtssache Akerberg/Fransson der Fall, wo es um Mehrwertsteuerbetrug ging und der EuGH daher die Grundrechtecharta für anwendbar hielt, [40] obwohl selbst der Generalanwalt in dieser Sache den EuGH nicht für zuständig gehalten hatte.

Das BVerfG wiederum hat in seiner Entscheidung zur Antiterrordatei vom 24.4.2013[41] angemerkt, dass der EuGH keine allgemeinen Aussagen treffen wollte, sondern es nur um seine Zuständigkeit für Grundrechtsfragen im Zusammenhang mit dem europäisch geregelten Umsatzsteuerrecht ging. Allerdings geht dann das BVerfG im Urteil ungewöhnlich ausführlich darauf ein, dass es keinen Anlass für ein Vorabentscheidungsverfahren vor dem EuGH gebe, da das Antiterrordateigesetz keine Durchführung europäischen Rechts i.S.v. Art. 51 Abs. 1 S. 1 GR-Charta sei. Das ist zwar in der Sache richtig. Das Vorgehen deutet aber auf Abgrenzung hin. Für den Datenschutz gemäß der DS-GVO kann es in Zukunft zu einer Doppelzuständigkeit kommen: der EuGH ist zuständig, soweit es um „Durchführung des Rechts der Union“ geht, also im harmonisierten Bereich. In den Bereichen, wo die DS-GVO eine Öffnung für nationale Regelungen enthält, sieht es anders aus. Sofern der nationale Gesetzgeber von den Regelungsoptionen Gebrauch macht, handelt es sich gerade nicht um harmonisiertes Recht und

30 BVerfGE 73, 339, 377; BVerfGE 102, 147, 164.
31 BVerfGE 89, 155, 188.
32 BVerfGE 123, 267, 340 ff.
33 BVerfGE 123, 267, 358 ff.
34 Vgl. dazu auch *Dederer*, JZ 2014, 313, der die These vertritt, dass sich die drei Prüfungsmaßstäbe des BVerfG harmonisieren lassen.
35 *Heuschmid/Lörcher,* NK-GA, Art. 51 Rn. 9 ff.
36 *Masing*, JZ 2015, 477, 480.
37 A.a.O., S. 481.
38 *Grimm*, JZ 2013, 585, 590 f.
39 A.a.O.
40 EuGH, Urt. v. 26.2.2013 – C-617/10, NJW 2013, 1415 (Akerberg/Fransson).
41 BVerfG, Urt. v. 24.4.2013, 1 BvR 1215/07, NJW 2013, 1499 Rn. 91.

es bleibt bei der Zuständigkeit des BVerfG.[42] Allerdings muss der EuGH überprüfen können, ob sich die nationale Regelung, die nur aufgrund der Verordnung überhaupt zulässig ist, im Bereich der Verordnung hält.[43]

II. Herausforderungen an die Neuregelungen

Die im Wesentlichen drei Herausforderungen an die Neuregelung sind schwer zu erfüllen. Naturgemäß ist bei der Bewertung, inwieweit den eigenen Ansprüchen Genüge getan wurde, der politische Blick auf die Einigung in der Grundverordnung milder[44] als der nüchterne Blick der Fachöffentlichkeit.

Hauptanspruch der DS-GVO ist es, in allen 28 Mitgliedstaaten einen einheitlichen Datenschutzstandard zu schaffen, nicht zuletzt um die digitale Wirtschaft in der EU zu beflügeln. Entsprechend stellt Art. 1 DS-GVO Datenschutz und Datenfreiheit als ein einheitliches Ziel dar. Nach Art. 1 Abs. 1 enthält die Verordnung Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, aber auch für den Schutz des freien Datenverkehrs in der Union.

Darüber hinaus soll ein moderner Datenschutz geschaffen werden, wobei weitgehend unklar bleibt, was mit „modern" genau gemeint ist. Schließlich soll der Datenschutz in Zukunft technikneutral ausgestaltet sein, um mit den rasant weiterentwickelten Informations- und Kommunikationstechnologien Schritt halten zu können.

Die DS-GVO soll wegen der Verordnungswirkung in Art. 288 Abs. 2 S. 2 AEUV zu einer deutlichen Vereinheitlichung des Datenschutzniveaus in den 28 Mitgliedstaaten führen. Anders als bei der Datenschutzrichtlinie vom 24.10.1995, die auch die geregelte Rechtsmaterie harmonisieren will, gibt es bei einer Verordnung kein Umsetzungserfordernis und damit auch keinen entsprechenden Spielraum. Bei der europäischen Datenschutzrichtlinie hatte der dazu geführt, dass die nationalen Vorgaben zum Datenschutzrecht sehr unterschiedlich blieben,[45] sodass sich nicht nur Unternehmen wie Google oder Facebook einen datenschutzgenehmen Standort innerhalb der EU aussuchen konnten.

Schließlich trägt zu einer vereinheitlichenden Wirkung auch der weite Anwendungsbereich der DS-GVO bei. Die nach Art. 3 Abs. 1 DS-GVO für die Datenverarbeitung von Unternehmen gültige Verordnung wendet, anders als die DS-Richtlinie mit dem Territorialitätsprinzip, das Sitz- sowie das Marktortprinzip an. Hiernach werden einerseits Unternehmen erfasst, die eine Niederlassung in der EU haben, unabhängig davon, ob die Datenverarbeitung innerhalb oder außerhalb der EU stattfindet. Andererseits muss das EU-Datenschutzrecht gemäß Art. 3 Abs. 2 DS-GVO aber auch von Unternehmen beachtet werden, die – auch ohne Niederlassung in einem Mitgliedstaat – in der EU entgeltlich oder unentgeltlich Waren oder Dienstleistungen anbieten und dazu Daten von Personen innerhalb der EU verarbeiten. Damit werden auch Unternehmen aus dem EU-Ausland von der DS-GVO erfasst, was vor allem für US-amerikanische Unternehmen, die innerhalb der EU aktiv sind, eine Änderung bedeuten wird, da deren Datenerhebung und –verarbeitung ab Mai 2018 an europäischem Datenschutzrecht gemessen wird. Ganz fremd war das Marktortprinzip aber auch unter der Geltung der Datenschutzrichtlinie nicht, da der EuGH in jüngerer Zeit diesem Prinzip in seiner Rechtsprechung z.T. bereits Geltung verschafft hatte.[46]

42 Vgl. auch NK-GA, Art. 23 ff.; *Kingreen*, JZ 2013, 801; BVerfG, Urt. v. 15.12.2015 - 2 BvR 2735/14, NJW 2016, 1149.
43 Hierbei wird es vor allem um die Auslegung von Art. 88 Abs. 2 DS-GVO gehen. Dazu unten E.II.2.
44 *Maas,* DuD 2015, 579; *Albrecht*, CR 2016, 88; *ders.*, ZD 2013, 587.
45 Vgl. EuGH, Urt. v. 24.11.2011 – C-468/10, C-469/10, RDV 2012, 22 (ASNEF).
46 So etwa in der Google Spain-Entscheidung, dazu *Kühling*, EuZW 2014, 527.

III. Prinzipien und Instrumente der DS-GVO

Die DS-GVO hat gemäß Art. 1 Abs. 1 nicht nur den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, also deren informationelle Selbstbestimmung zum Ziel, sondern gleichgewichtig auch das Gegenteil, nämlich gerade den freien Verkehr solcher Daten. Der darf sogar nach Art. 1 Abs. 3 nicht allein mit der Begründung eingeschränkt werden, es gehe um den Schutz natürlicher Personen bei der Verarbeitung von deren personenbezogener Daten. Der freie Datenverkehr erhält damit einen ebenso hohen wie der Persönlichkeitsschutz. Für die zukünftige Auslegung der DS-GVO dürfte das bedeuten, dass immer eine Interessenabwägung zwischen diesen beiden Polen stattzufinden hat. Die bisherige grundrechtliche Perspektive des deutschen Datenschutzrechts kollidiert mit dem europarechtlichen Spannungsverhältnisses zwischen Grundrechten und Grundfreiheiten. Die „historisch bedingte Schieflage“[47] zugunsten der Förderung des Binnenmarktes und also zugunsten der Grundfreiheiten hat erst durch die verbindliche Verankerung der GR-Charta als Primärrecht in Art. 6 Abs. 1 EUV und die Aufnahme von sozialer Marktwirtschaft und sozialem Fortschritt als Ziele der Union in Art. 3 Abs.3 S. 2 EUV etwas mehr Balance erhalten. Ob dadurch EuGH-Bewertungen wie in den Fällen *Viking*[48] und *Laval,*[49] in denen das Grundrecht auf Koalitionsfreiheit zugunsten der Grundfreiheiten des freien Dienstleistungsverkehrs bzw. der Niederlassungsfreiheit zurückstehen musste, beim Datenschutz in Zukunft grundrechtsorientierter ausfallen werden, bleibt abzuwarten. Erste Entscheidungen des EuGH aus jüngerer Zeit deuten in die richtige Richtung.[50]

Im Übrigen führt die DS-GVO nicht grundsätzlich zu einer völligen Umwertung des Datenschutzes, denn sie gründet nicht nur auf ihrer 20 Jahre alten Vorgängerin, der EU-Datenschutzrichtlinie, sondern nimmt auch Strukturen aus den nationalen Datenschutzbestimmungen der Mitgliedstaaten auf, nicht zuletzt auch den deutschen. Daher werden die Auswirkungen der DS-GVO für Unternehmen in Deutschland auch für „überschaubar“ gehalten.[51] So geht auch die DS-GVO von einem weiten Datenverarbeitungsbegriff aus (Art. 2 Abs. 1), der sowohl die automatisierte wie die nicht automatisierte Verarbeitung personenbezogener Daten umfasst – analoge Daten sind allerdings nicht gemeint -, wobei auch in der DS-GVO der Streit über den absoluten (objektive, technische Bestimmbarkeit des Personenbezuges) oder relativen Personenbezug (subjektive Möglichkeit des Datenverarbeiters, den Personenbezug herzustellen) nicht geklärt wird.[52]

Begrifflich wird im Verordnungstext nicht zwischen Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten unterschieden, wie in § 1 Abs. 2 BDSG, sondern es ist einheitlich von „Verarbeitung“ solcher Daten die Rede, Art. 1 Abs. 1 DS-GVO. Dieser Verarbeitungsbegriff ist aber weit gemeint, wie die Definitionsnorm Art. 4 Nr. 2 DS-GVO deutlich macht. Danach umfasst der Begriff „Verarbeitung“ nicht nur das bisherige Erheben, Verarbeiten und Nutzen von personenbezogenen Daten, sondern „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang“, wozu u.a. auch Organisation, Ordnen, Anpassung oder Veränderung, Auslesen, Abfragen, Abgleich und Verknüpfung personenbezogener Daten gehören.

Darüber hinaus findet sich der wesentliche Grundsatz des Datenschutzes in § 4 Abs. 1 BDSG, das Verbot mit Erlaubnisvorbehalt, auch in der Verordnung (Art. 6 Abs. 1), wonach die

47 *Pötters*, Grundrechte und Beschäftigtendatenschutz, 2013, S. 259.
48 EuGH, Urt. v. 11.12.2007 – C-438/05, Slg. 2007, I-10779 (Viking).
49 EuGH, Urt. v. 18.12.2007 – C-341/05, Slg. 2007, I-11767 (Laval).
50 EuGH, Urt. v. 8.4.2014 – C-293/12, C-594/12, DuD 2014, 488 (Vorratsdatenspeicherung); EuGH, Urt. v. 13.5.2014 – C-131/12, DuD 2014, 559 (Google); EuGH, Urt. v. 6.10.2015 – C-362/14, DuD 2015, 823 (Safe Harbor). Vgl. dazu auch noch unten C.VII.2.b).
51 U.a. *Kraska*, ZD-Aktuell 2016, 04173.
52 *Kort*, DB 2016, 711.

Verarbeitung personenbezogener Daten im Prinzip verboten ist und erst durch einen Erlaubnistatbestand, vor allem eine gesetzliche Regelung, eine Einwilligung[53] oder eine der weiteren in Art. 6 genannten Verarbeitungszusammenhänge gerechtfertigt werden muss. Dazu gehört die Verarbeitung zur Erfüllung eines Vertrages der betroffenen Person (Art. 6 Abs. 1 lit. a) oder zum Schutz lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person (Art. 6 Abs. 1 lit. d). Bei der Verarbeitung zur Erfüllung rechtlicher Verpflichtungen des Verantwortlichen (Art. 6 Abs. 1 lit. c) oder für die Wahrnehmung einer Aufgabe im öffentlichen Interesse (Art. 6 Abs. 1 lit. e) eröffnet Art. 6 Abs. 2 DS-GVO den Mitgliedstaaten die Möglichkeit „spezifischere Bestimmungen" zu erlassen. In der Liste der Verarbeitungsgründe ist Art. 6 Abs. 1 lit. f der problematischste, denn er erlaubt die Verarbeitung im berechtigten Interesse des Verantwortlichen.[54] Darüber hinaus können auch berechtigte Interessen Dritter Datenerhebung und -verarbeitung rechtfertigen, eine Vorschrift, die im Laufe des Gesetzgebungsverfahrens sehr umstritten war, sich aber im Trilog schließlich durchsetzen konnte.[55] Zwar muss im Vergleich zur Datenschutzrichtlinie von 1995 zumindest eine Abwägung mit den „Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person" erfolgen. Kriterien für diese Abwägung enthält die DS-GVO aber nicht. Art. 6 Abs. 1 lit. f DS-GVO wird wohl der Maßstab für neue Geschäftsmodelle im Internet werden.

Auch am Zweckbindungsgrundsatz, dem Leitprinzip des Datenschutzes, das aber im BDSG nicht klar kodifiziert ist,[56] hält die DS-GVO in Art. 5 Abs. 1 lit. b fest, wonach personenbezogene Daten nur für die zuvor festgelegten legitimen Zwecke erhoben und weiterverarbeitet werden dürfen. In Art. 6 Abs. 2 erlaubt die DS-GVO für bestimmte Datenverarbeitungserlaubnisse nationale Verschärfungen. Allerdings sind nach Art. 6 Abs. 4 DS-GVO unter bestimmten Voraussetzungen spätere Zweckänderungen erlaubt. Hierunter dürften – im Prinzip – Big Data-Anwendungen fallen, bei denen große Datenmengen zunächst zweckfrei gesammelt werden, um durch spätere Auswertungen neue Kenntnisse zu generieren.[57] Auch der aus § 3a S. 2 BDSG bekannte Grundsatz der Datenvermeidung und Datensparsamkeit, der gemäß BDSG durch Anonymisierung und Pseudonymisierung gewährleistet werden soll, taucht in Art. 5 Abs. 1 lit. c DS-GVO wieder auf, wenn auch vager: die Datenerhebung soll auf das notwendige Maß beschränkt werden.

Eine Sonderstellung nehmen die sensiblen Daten gemäß Art. 9 DS-GVO ein. Schon in § 3 Abs. 9 BDSG sind weitgehend dem Allgemeinen Gleichbehandlungsgesetz (AGG) entsprechende Merkmale definiert, deren Erhebung und Verarbeitung nach § 28 Abs. 6–9 BDSG strengeren Verarbeitungsvoraussetzungen unterliegen als sonstige personenbezogene Daten. Diesen Ansatz greift Art. 9 DS-GVO auf und regelt im Großen und Ganzen sogar strenger als das deutsche Recht. So dürfen die in Art. 9 Abs. 1 aufgezählten sensiblen Daten nach Abs. 3 nur von Fachpersonal verarbeitet werden, das einer Geheimhaltungspflicht unterliegt. Diese Einschränkung gilt nach § 28 Abs. 7 BDSG nur für Gesundheitsdaten.[58]

Daneben enthält die DS-GVO weitere Instrumente, wie umfangreichere Informationspflichten als im BDSG in Art. 13 f. oder hohe Transparenzanforderungen in Art. 12. Allerdings muss bedacht werden, dass es angesichts der unübersehbaren Menge an Daten, die bei

53 Dazu näher für den Beschäftigungskontext unten E.III.4.

54 Kritisch *Roßnagel/Nebel/Richter*, ZD 2015, 455, 457.

55 Zur Kritik *Roßnagel/Kroschwald*, ZD 2014, 45, 499; gefordert worden war die Berücksichtigung von Drittinteressen u.a. von *Gola/Schulz*, RDV 2013, 1, 6, 7.

56 *Kühling/Seidel/Sivridis*, Datenschutzrecht, 2015, 3. Auflg., Rn. 286.

57 Kritisch zur Ausgestaltung des Zweckbindungsgrundsatzes in der DS-GVO schon zum Ratsentwurf: *Richter*, DuD 2015, 735, 740.

58 Näher zu Art. 9 DS-GVO im Beschäftigungszusammenhang noch unten E.II.2.d) und mit Bezug zur Einwilligung unter E.III.4.d)bb).

der IT-Nutzung im nicht-öffentlichen Bereich laufend entsteht, zwar rechtlich möglich ist, Transparenzanforderungen festzulegen, faktisch aber unmöglich sein wird, eine umfassende Transparenz zu schaffen (und zu kontrollieren). In Bezug auf bestimmte Daten oder/und gegenüber bestimmten Akteuren, wie etwa im Beschäftigtendatenschutz, mag sich das jedoch eher realisieren lassen.[59]

Von eher anekdotischem Wert ist der Werdegang des „Rechts auf Vergessenwerden" in Art. 17 DS-GVO. Das im Kommissionsentwurf mit großem Marketingaufwand beworbene Recht auf Vergessenwerden[60] war von vornherein nur ein Löschungsrecht, wie es schon existiert. Das Europäische Parlament hatte Art. 17 daher konsequenterweise mit „Recht auf Löschung" überschrieben, der Rat griff auf die ursprüngliche Version (in Anführungsstrichen) zurück und in der verabschiedeten Fassung heißt es nun „Recht auf Löschung („Recht auf Vergessenwerden")". Selbst ein solches (bescheidenes) Löschungsrecht wird im privaten Bereich kaum umfassend, sondern allenfalls bereichsspezifisch wirkungsvoll umsetzbar sein. Was es konkret bedeutet, hat der EuGH bereits in der Google-Spain-Entscheidung festgelegt:[61] auf eine für den Betroffenen negative Information, die für die Öffentlichkeit nicht (mehr) von Interesse ist, darf eine Suchmaschine nicht mehr hinweisen. Das heißt aber nicht, dass die Information nicht mehr auffindbar ist. Im entschiedenen Fall blieb die ungünstige Information im fraglichen Register enthalten.

Die DS-GVO formuliert als eines von zwei Hauptzielen neben der Modernisierung des Datenschutzes die Vereinheitlichung der Regeln in allen Mitgliedstaaten. Dem dienen die o.a. für alle 28 Mitgliedstaaten einheitlichen gesetzlichen Erlaubnistatbestände für Datenerhebung und –verarbeitung. Zusätzlich können natürlich auch andere EU-Normen Erlaubnistatbestände i.S. des Grundsatzes Verbot mit Erlaubnisvorbehalt sein. Ob, wie und wann es möglich sein wird, aus derartigen Generalklauseln den mit der Verordnung anvisierten einheitlichen europäischen Datenschutz zu schaffen bleibt abzuwarten. Das Ziel dürfte allerdings schon allein aufgrund der zahlreichen Öffnungsklauseln nicht erreichbar sein.

Wegen der entsprechenden Schwierigkeiten und der mit unbestimmten Rechtsbegriffen einhergehenden Rechtsunsicherheit, war bislang anerkannt, dass effizienter Datenschutz am besten mit bereichsspezifischen Regelungen zu erzielen ist,[62] da generalklauselartige Regeln zwar eine Vielzahl von Fällen erfassen können, jedoch den spezifischen Datenverarbeitungsbedingungen in sehr unterschiedlichen Zusammenhängen nicht gerecht werden. Entsprechend haben im deutschen Datenschutzrecht gemäß § 1 Abs. 3 BDSG spezialgesetzliche Rechtsvorschriften zum Datenschutz Vorrang vor dem BDSG. Dieses allgemeine Subsidiaritätsprinzip ist in der DS-GVO nicht mehr vorhanden, was z.T. in der Literatur für einen Paradigmenwechsel gehalten wird,[63] der die Frage aufwirft, was aus dem bisherigen bereichsspezifischen deutschen Datenschutzrecht, etwa dem GenDG oder den Datenschutznormen des SGB wird. Vor diesem Hintergrund sind die ca. zehn Regelungsaufträge an den nationalen Gesetzgeber (insbesondere zur Aufsicht) und ca. 30 Regelungsoptionen,[64] darunter zum Beschäftigtendatenschutz, zu begrüßen.

Diese Öffnung für nationale Regelungen, insbesondere in brisanten Bereichen, war zunächst nicht geplant. Die Fortentwicklung des Datenschutzes sollte bei der Kommission

59 *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 121 ff., 133 ff.

60 Kritisch schon zum Kommissionsvorschlag *Körner,* ZESAR 2013, 99 ff. und 153 ff.; richtig hat *Grimm* angemerkt, dass ein solches Recht jenseits rechtlicher Gewährleistungsmöglichkeiten liegt, a.a.O., S. 589.

61 EuGH, Urt. v. 13.5.2014 – C-131/12, NJW 2014, 2257.

62 *Simitis*, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 2014, 8. Auflg., Einleitung Rn. 20, 32.

63 *Brink*, in: Boecken/Düwell/Diller/H.Hanau (Hrsg.), Nomos-Kommentar Gesamtes Arbeitsrecht, 2016, 1. Auflg., § 32 BDSG Rn 22.

64 Einige davon genannt bei *Buchner*, DuD 2016, 155, 160 und bei *Kraska*, ZD-Aktuell 2016, 04173.

zentralisiert werden, die in sog. delegierten Rechtsakten jeweils Regelungen zu speziellen Verarbeitungszusammenhängen hätte erlassen dürfen, auch im Beschäftigtendatenschutz. Dabei hätte es sich dann nach Art. 290 AEUV um verbindliche exekutive Rechtsetzung gehandelt.[65] Dieser Plan wurde fallengelassen. Nur noch in zwei Fällen darf die Kommission delegierte Rechtsakte erlassen: gemäß Art. 40 Abs. 9 und Art. 12 Abs. 8 DS-GVO.

Das erlaubt den Mitgliedstaaten in einem unerwartet weiten Umfang doch noch ihre nationalen Vorstellungen von Datenschutz umzusetzen. Der Preis ist allerdings, dass es keinen einheitlichen Datenschutz in allen Mitgliedstaaten geben wird. Ähnliches kennt man schon von der Europäischen Aktiengesellschaft (SE), wo es keine EU-einheitliche europäische Aktiengesellschaft gibt, sondern 28 verschiedene Gesellschaften, da an zahlreichen Stellen auf das nationale Recht zurückgegriffen wird.[66] Faktisch nimmt die DS-GVO damit eine Zwitterstellung zwischen Verordnung und Richtlinie ein, was zu weniger statt mehr Rechtsangleichung beim Datenschutz führt. Je nachdem, in welchem Umfang die Mitgliedstaaten von den Regelungsbefugnissen Gebrauch machen, wird die Unübersichtlichkeit der Datenschutzregelungen in den 28 Staaten zwar z.T. abgebaut, aber nicht beseitigt werden, was sich auch auf den Grundrechtsschutz auswirkt.[67]

IV. Betroffenenrechte

Die Betroffenenrechte in Art. 13 ff. DS-GVO entsprechen im Wesentlichen dem bekannten System,[68] sind sogar z.T. weitgehender als die in §§ 33-35 BDSG geregelten. Sie umfassen Informationsrechte (Art. 13 f.), Löschungsrechte (Art. 17), die Datenübertragbarkeit (Art. 20) und Widerspruchsrechte (Art. 21). Da die DS-GVO vor allem die Transparenz der Datenverarbeitung erhöhen will, sind die Informationsrechte des Betroffenen in Art. 13 und 14 deutlich weiter gefasst als im BDSG. Neben Pflichtinformationen, wie zur verantwortlichen Datenverarbeitungsstelle, über die Zwecke der Verarbeitung, die berechtigten Interessen eines Dritten i.S.v. Art. 6 Abs. 1 lit. f und die Absicht des Verantwortlichen, Daten in ein Drittland zu übermitteln, gibt es fakultative Informationspflichten, die erfüllt werden müssen, wenn sie für eine transparente Datenverarbeitung erforderlich sind. Hierzu zählen u.a. die Kriterien für die Festlegung der Dauer der Datenspeicherung oder die Quellen der Daten. Im Bereich der Informationsrechte des Betroffenen hat die Kommission eine ihrer im Vergleich zum DS-GVO-Entwurf von 2012 zahlenmäßig stark reduzierten Befugnisse für den Erlass delegierter Rechtsakte behalten. Gemäß Art. 12 Abs. 8 DS-GVO darf sie entsprechend vorschreiben, die Information im Wege standardisierter Bildsymbole zu erteilen.

Die Löschungsrechte dagegen gehen nicht viel weiter als schon nach dem BDSG, zumal das „Recht auf Vergessenwerden" in Art. 17 Abs. 2 DS-GVO, wenn es auch begrifflich neu ist, nur bedeutet, dass der Verantwortliche, der personenbezogene Daten öffentlich gemacht hat (i.d.R. im Internet), andere Stellen, die die Daten weiterverarbeiten, darüber informieren muss, dass ein Betroffener die Löschung von Links zu diesen personenbezogenen Daten verlangt hat, wobei diese Pflicht durch Implementierungskosten des Verpflichteten relativiert wird.

Neu ist dagegen das unterhalb des Löschungsrechts angesiedelte Recht auf Einschränkung der Verarbeitung in Art. 18 DS-GVO. Die vier genannten, abschließenden Voraussetzungen betreffen Situationen, in denen der Betroffene zwar (noch) keine Löschung, aber die

65 Sog. „tertiäres Unionsrecht", *Kühling/Seidel/Sivridis*, Datenschutzrecht, 2015, 3. Auflg., Rn. 141.
66 Vgl. Art. 9 SE-VO.
67 Dazu schon oben C.I.3.
68 Ausführlich beschrieben von *Franck*, RDV 2016, 111.

Einschränkung der Verarbeitung seiner personenbezogenen Daten wünscht. Dies ist z.B. der Fall, wenn die betroffene Person die Richtigkeit ihrer Daten bestreitet, dieser Umstand aber noch geprüft werden muss (Art. 18 Abs. 1 lit. a) oder wenn der Verantwortliche die Daten für den Verarbeitungszweck nicht mehr benötigt, die betroffene Person sie aber zur Ausübung von Rechtsansprüchen noch braucht (Art. 18 Abs. 1 lit. c).

Eine problematische Seite hat das Recht auf Datenübertragbarkeit in Art. 20 DS-GVO. Damit soll Betroffenen vor allem ermöglicht werden, ihre Profile in sozialen Netzwerken oder ihre E-Mail-Konten zu anderen Anbietern mitzunehmen. Art. 20 erlaubt daher, ihre personenbezogenen Daten in einem „strukturierten, gängigen und maschinenlesbaren Format" zu erhalten. Zum Problem für den Datenschutz Dritter kann dieses Betroffenenrecht deshalb werden, weil bei der Übertragung von Profilen oder E-Mail-Konten unvermeidlich auch Daten Dritter mitübertragen werden, etwa empfangene Mails oder Chat-Verläufe.[69]

Erwägungsgrund 59 der DS-GVO verweist schließlich darauf, dass die Betroffenenrechte unentgeltlich ausgeübt werden sollen, Anträge auch elektronisch gestellt werden dürfen und der Verantwortliche „verpflichtet werden sollte" innerhalb eines Monats zu antworten, allerdings nur „gegebenenfalls" mit einer Begründung. Sind diese Anforderungen schon etwas vage formuliert, so bleibt abzuwarten, inwieweit die Mitgliedstaaten von den Regelungsbefugnissen nach Art. 23 DS-GVO Gebrauch machen werden. Bei Art. 23 handelt es sich um eine der Öffnungsklauseln, nach denen die Mitgliedstaaten ausdrücklich Beschränkungen der Verordnung einführen dürfen. Zwar sollen solche Beschränkungen „den Wesensgehalt der Grundrechte und Grundfreiheiten achten und eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme" darstellen, jedoch reicht die Liste der Gründe, aus denen Einschränkungen erlaubt sind von der nationalen (Art. 23 Abs. 1 lit. a) über die öffentliche Sicherheit (Art. 23 Abs. lit. c), den Schutz „sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses" (Art. 23 Abs. 1 lit. e) bis zur Durchsetzung zivilrechtlicher Ansprüche" (Art. 23 Abs. 1 lit. j).

V. Datenschutz-Folgenabschätzung

Im Vergleich zur Vorabkontrolle nach § 4d Abs. 5 BDSG neu und weitreichender ist die Pflicht des Datenverarbeiters zur Datenschutz-Folgenabschätzung nach Art. 35 Abs. 1 DS-GVO. Diese besteht, wenn die Form der Verarbeitung, vor allem bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für Rechte und Freiheiten natürlicher Personen zur Folge hat. Beispielhaft sind die umfangreiche Verarbeitung sensibler Daten (Art. 35 Abs. 3 lit. b) oder die systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche (Art. 35 Abs. 3 lit. c) genannt. Dann muss gemäß Art. 36 DS-GVO eine vorherige Konsultation mit der Aufsichtsbehörde stattfinden. Eine Vorab-Genehmigungspflicht bedeutet das nicht, aber die Aufsichtsbehörde kann schriftliche Empfehlungen abgeben (Art. 36 Abs. 2 DS-GVO). Außerdem bleiben ihre sonstigen Aufsichts- und Abhilfebefugnisse nach Art. 58 DS-GVO[70] unberührt.

In den Regelungen über die Folgenabschätzung werden z.T. „Informationsmöglichkeiten" für den Betriebsrat gesehen.[71] Ein rechtlicher Anspruch hinsichtlich des durch die DS-GVO neu geschaffenen Instruments der Datenschutz-Folgenabschätzung ergibt sich allerdings weder aus den allgemeinen Informationsrechten des Betriebsrats nach dem BetrVG (§§ 75 und

69 Das hält *Schantz*, NJW 2016, 1841, 1845 für unproblematisch, da das Recht auf Datenübertragbarkeit sonst leer liefe.
70 Zur Aufsicht unten C.VII.
71 *Wedde*, CuA 2016, 8 ff.

80) noch aus der DS-GVO direkt.[72] Die enthält in Art. 35 Abs. 2 eine ausdrückliche Regelung im Zusammenhang mit der DatenschutzFolgenabschätzung nur zum Datenschutzbeauftragen. Sofern vorhanden, muss der Datenschutzbeauftragte konsultiert werden.

VI. Durchsetzung und Sanktionen

Zum Zwecke der Durchsetzung der DS-GVO und der Sanktionierung von Verstößen wurden Meldepflichten, Beschwerderechte der Betroffenen, Bußgelder, Haftung und Schadensersatz sowie ein Verbandsklagerecht geregelt. In diesem Bereich gibt es auch etliche Regelungsaufträge an die nationalen Gesetzgeber, etwa zur Festlegung weiterer Sanktionsarten in Art. 84 DS-GVO. Für Deutschland bedeutet das, dass die strafrechtlichen Sanktionen in § 44 Abs. 1 BDSG beibehalten werden könnten.

Die Dokumentationspflicht in § 4g Abs. 2 i.V.m. § 4e BDSG wird in Art. 28 DS-GVO aufgegriffen und vergleichbar geregelt.[73] Weiter als § 42a BDSG regeln Art. 31 und 32 DS-GVO Meldepflichten bei Datenschutzverstößen, wobei allerdings durch technische und organisatorische Maßnahmen die Meldepflicht entfallen kann.

Bußgelder nach § 43 BDSG wurden bislang eher zurückhaltend verhängt, von einzelnen Ausnahmen, wie der Geldbuße in Höhe von ca. 1,5 Millionen Euro für die Supermarktkette Lidl im Jahre 2008 abgesehen,[74] die Verstöße gegen den Beschäftigtendatenschutz betraf.[75] Nun wird in der DS-GVO der Rahmen für Bußgelder an das Kartellrecht angelehnt und in Art. 83 Abs. 4 DS-GVO deutlich auf bis zu 10 Millionen Euro oder bei Unternehmen auf bis zu 2% des weltweiten Jahresumsatzes erhöht. Bei Verstößen gegen die Verarbeitungsgrundsätze der DS-GVO – ausdrücklich auch bei Verstößen gegen die Voraussetzungen einer rechtmäßigen Einwilligung –, bei Verstößen gegen die Betroffenenrechte und bei Missachtung von Anweisungen der Aufsichtsbehörden kann gemäß Art. 83 Abs. 5 DS-GVO das Bußgeld sogar bis zu 20 Millionen Euro oder 4% des Jahresumsatzes betragen. Allerdings könnte diese Bußgeldhöhe eher symbolischen Wert haben. Zum einen funktioniert diese Abschreckung nur bei effizienter Aufsicht, deren Verfahren sehr komplex geregelt ist. Zum anderen ist zweifelhaft, ob entsprechende Beträge je verhängt würden, da die Aufsichtsbehörden ein erhebliches Prozessrisiko tragen würden. Allerdings wird in der Diskussion um die Auswirkungen der DS-GVO gerade von Unternehmensseite immer wieder auf die Risiken durch die hohen Bußgelder verwiesen[76] und in der Bußgeldregelung gar die praxisrelevanteste Neuerung der DS-GVO gesehen.[77] Verhängt werden könnten die hohen Bußgelder jedenfalls im Prinzip auch bei Verstößen gegen den Beschäftigtendatenschutz.

Neben den staatlichen Bußgeldern könnte in Zukunft die zivilrechtliche Haftung mit Schadensersatzansprüchen bei der Sanktionierung von Datenschutzverstößen eine größere Rolle spielen. Eine Schadensersatznorm enthält zwar auch schon § 7 BDSG, der Art. 23 der EG-Datenschutzrichtlinie umsetzt und sowohl für schuldhafte Datenschutzverstöße von öffentlichen wie nichtöffentlichen Stellen gilt. Nur für öffentliche Stellen regelt § 8 BDSG zusätzlich

72 Zur Rolle des Betriebsrats siehe unten E.IV.1.

73 *Gierschmann*, ZD 2016, 51, 53.

74 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, Dem Datenschutz wachsen Zähne, Pressemitteilung 11.9.2008, abrufbar unter: www.datenschutzzentrum.de/presse/20080911-lidl-bussgeldverfahren.html (abgerufen am 6.7.2016).

75 § 32 BDSG gab es da allerdings noch nicht. Diese Norm war gerade die gesetzgeberische Reaktion u.a. auf den Lidl-Fall.

76 *Faust/Spittka/Wybitul*, ZD 2016, 120.

77 *Ashkar*, DuD 2015, 796, 799.

eine verschuldensunabhängige Gefährdungshaftung. Der Schadensersatzanspruch spielt auch deshalb bislang, vor allem bei Unternehmen, in der Praxis so gut wie keine Rolle.[78]

Eine verschuldensunabhängige Haftung führt zwar auch die DS-GVO nicht ein (Art. 82 Abs. 3). Dennoch bringt Art. 82 DS-GVO zwei Verbesserungen im Vergleich zur derzeitigen Rechtslage. Zum einen wird eine Regelungslücke des bisherigen Rechts geschlossen, indem nicht nur der Verantwortliche, sondern gemäß Art. 82 Abs. 2 auch der Auftragsdatenverarbeiter haftet, wenn auch beschränkt auf die Nichteinhaltung der ihm auferlegten Pflichten aus der Verordnung bzw. der rechtmäßig erteilten Anweisungen des Verantwortlichen. Verantwortlicher und Auftragsdatenverarbeiter haften nach Art. 82 Abs. 4 als Gesamtschuldner, können sich also gegenüber dem Geschädigten nicht auf den jeweils anderen Verarbeitungszusammenhang berufen. Zum anderen ist gemäß Art. 82 Abs. 1 nicht nur der materielle, sondern auch der immaterielle Schaden zu ersetzen. Nach deutschem Recht ist der Ersatz immaterieller Schadens bei einer Datenschutzverletzung nur ausnahmsweise bei besonders schwerer Verletzung des allgemeinen Persönlichkeitsrechts zu gewähren. Diese Einschränkung wird in Zukunft nicht mehr möglich sein. Das gilt auch für den im Rahmen von Art. 88 DS-GVO national geregelten Beschäftigtendatenschutz, denn Erwägungsgrund 146 stellt klar, dass als Verstöße gegen die DS-GVO, die Schadensersatzansprüche auslösen können, auch Verstöße gegen Rechtsvorschriften der Mitgliedstaaten gelten, die aufgrund der DS-GVO erlassen wurden. Das bedeutet, dass ein Verstoß gegen einen im Rahmen von Art. 88 Abs. 3 DS-GVO[79] der Kommission gemeldeten § 32 BDSG die Schadensersatzansprüche (und auch die Bußgeldhöhen) der Verordnung auslöst.

Wie sich schließlich der immaterielle Schadensersatzanspruch in der europäischen Rechtspraxis konkret darstellen wird, bleibt abzuwarten. Jedenfalls sind die Kriterien europarechtsautonom auszulegen. In den Mitgliedstaaten ist der Umgang mit immateriellem Ersatz sehr unterschiedlich. Insbesondere in Deutschland sind die Ersatzbeträge niedrig. Erwägungsgrund 146 verlangt „vollständigen und wirksamen“ Schadensersatz und verweist für die Bemessung des Ersatzes auf die Rechtsprechung des EuGH. Der betont, dass zivilrechtliche Sanktionen abschreckend sein müssen.[80]

Kapitel VIII der DS-GVO über Haftung und Sanktionen erleichtert den Rechtsweg für Betroffene bei ihren Klagen gegen Verantwortliche oder Auftragsdatenverarbeiter. Nach Art. 79 Abs. 2 DS-GVO i.V.m. Erwägungsgrund 145 bleibt es dem Betroffenen überlassen, ob er die Gerichte des Mitgliedstaates anruft, in dem der Verantwortliche oder der Auftragsdatenverarbeiter eine Niederlassung hat oder in dem die betroffene Person ihren Aufenthaltsort hat. Von dieser Wahlfreiheit des Betroffenen gibt es nur eine Ausnahme für Behörden, die in Ausübung ihrer hoheitlichen Befugnisse handeln (Art. 79 Abs. 2, S. 2, Hs. 2).

Schließlich sieht die DS-GVO in Art. 80 Abs. 1 noch eine Art Prozessführungsbefugnis vor. Organisationen oder Vereinigungen ohne Gewinnerzielungsabsicht können von betroffenen Personen beauftragt werden, diese vor Aufsichtsbehörden oder Gerichten zu vertreten. Das geht weiter als der auch auf EU-Recht basierende § 23 Abs. 2 AGG, der die Möglichkeit einer Beistandschaft für Antidiskriminierungsverbände regelt, allerdings auf die Unterstützung in der mündlichen Verhandlung beschränkt ist und nach Abs. 3 nur die Möglichkeit eröffnet, bei der Formulierung von Klageanträgen zu unterstützen, ohne selbst als Vertreter aufzutreten.

Neben der Prozessführungsbefugnis in Art. 80 Abs. 1 eröffnet Art. 80 Abs. 2 DS-GVO für die Mitgliedstaaten die Möglichkeit, ein Verbandsklagerecht einzuführen.[81]

78 *Gola/Schomerus*, BDSG Kommentar, 2015, 12. Auflg., § 7 Rn 2.
79 Dazu genauer unten E.II.2.d).
80 Etwa EuGH, Urt. v. 17.12.2015, C-407/14,,EuZW 2016, 183 m.w.N. (Arjona Camacho).
81 Zur Verbandsklage unten E.IV.2.

VII. Aufsichts- und Auslegungsinstanzen

So wichtig umfassende materielle Regelungen zur Zulässigkeit von Datenverarbeitung und gestärkte Betroffenenrechte sind, kommt es für die Wirksamkeit der Regelungen auf die Durchsetzung, also auf die Vollzugsebene an. Die ist in der DS-GVO in den Kapiteln VI und VII über die Aufsichtsbehörden (Art. 51 ff.) und die Zusammenarbeit zwischen den Aufsichtsbehörden aus verschiedenen Mitgliedstaaten (Art. 60 ff.) geregelt. Der Umstand allein, dass die Regelungen Teil einer unmittelbar geltenden Verordnung sind, die Anwendungsvorrang vor nationalem Recht hat, stellt keine Garantie für eine wirkungsvolle Umsetzung dar, wie die Erfahrungen mit der 14 Jahre alten verbraucherschützenden Verordnung 2001/44/EG (EuGVVO) zeigen.[82]

1. Datenschutzbehörden, Art. 51 ff. DSGVO

Die Ausgestaltung der Datenschutzaufsicht, vor allem für die Fälle, in denen mehrere Mitgliedstaaten oder die ganze EU betroffen sind, war in den Verhandlungen zwischen Kommission, Parlament und Rat eines der umstrittensten Themen.[83]

Unter der Geltung der EG-Datenschutzrichtlinie erfolgt die Datenschutzaufsicht und –durchsetzung durch die Datenschutzbehörden der Mitgliedstaaten (Art. 28 Abs. 1 DS-RL 95/46/EG). Dabei hat nur Deutschland mit den Landes- und dem Bundesdatenschutzbeauftragten mehrere Aufsichtsbehörden. Sie sind auch für Unternehmen, also auch für den Beschäftigtendatenschutz zuständig.[84] Die Koordination der nationalen Datenschutzbehörden in den Mitgliedstaaten erfolgt bislang über Art. 28 Abs. 6 der Datenschutzrichtlinie und über die Art. 29-Datenschutzgruppe.[85] Für die Koordination innerhalb Deutschlands hat bislang der sog. Düsseldorfer Kreis diese Funktion. Der hat sich aber auch schon mit grenzüberschreitenden Problemen befasst und im Jahr 2010 eigene verschärfende Bedingungen für die Datenübertragung in Drittstaaten nach dem EU-USA-Safe-Harbor-Abkommen aufgestellt.[86]

Die Arbeit der Aufsichtsbehörden soll harmonisiert werden. Zunächst muss jeder Mitgliedstaat gemäß Art. 51 und 52 DS-GVO überhaupt erst einmal eine unabhängige Aufsichtsbehörde[87] schaffen. Die Rolle der Aufsichtsinstanzen im privaten Bereich verändert sich in der DS-GVO. Die externe Kontrolle von Unternehmen durch Aufsichtsbehörden ist im BDSG relativ eng geregelt, da das BDSG von der Vorstellung ausgeht, dass im Unternehmen der Grundsatz der Eigenkontrolle gilt, die vor allem durch den betrieblichen Datenschutzbeauftragten ausgeübt werden soll. Bei der Verantwortung der Unternehmen für den Datenschutz bleibt es zwar auch unter der Verordnung. Sie wird eher noch gestärkt durch die Datenschutz-Folgenabschätzung (Art. 35), Datenschutz durch Technik (Art. 25),[88] Zertifizierungen (Art. 42 f.) oder die Möglichkeit, die Aufsichtsbehörden vorab zu Rate zu ziehen (Art. 36). Letzteres darf aber nicht dazu führen, die Verantwortung für die Klärung von Compliance-Fragen auf die Aufsichtsbehörden zu verlagern.[89]

82 *Dieterich*, ZD 2016, 260, 263.
83 *Nguyen*, ZD 2015, 265.
84 Für das Telekommunikationsrecht (TKG und TMG) ist ausschließlich der Bundesdatenschutzbeauftragte zuständig.
85 *Dix*, DuD 2012, 318, 319.
86 *Düsseldorfer Kreis*, Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen, 2010.
87 Das war zwar auch schon unter der DS-Richtlinie so, aber gerade Deutschland musste sich erst vom EuGH ermahnen lassen, für die Unabhängigkeit seiner Aufsichtsbehörden zu sorgen: EuGH, Urt. v. 9.3.2010 – C-518/07 (Kommission/Deutschland), NJW 2010, 1265.
88 Dazu unten E.II.4.
89 So auch schon in der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Struktur der künftigen Datenschutzaufsicht in Europa, 87. Konferenz der Datenschutzbeauftragten, 27.3.2014, Nr. 6.

Die unternehmerische Verantwortung für den Datenschutz bleibt also bestehen und wird sogar erweitert. Allerdings werden daneben in Art. 57 DS-GVO die Aufgaben der externen Aufsichtsbehörden weiter gefasst. Deren Aufgabenkatalog ist im Vergleich zur DS-Richtlinie mit 22 Einzelaufgaben in Art. 57 Abs. 1 DS-GVO erheblich ausgedehnt worden und reicht von der Kernaufgabe Überwachung und Durchsetzung der DS-GVO (Art. 57 Abs. 1 lit. a) über die Aufklärung von Unternehmen zu datenschutzrechtlichen Pflichten (Art. 57 Abs. 1 lit. d) und die Bearbeitung von Anfragen und Beschwerden von Betroffenen (Art. 57 Abs. 1 lit. e und f) bis zur Genehmigung von Standardvertragsklauseln für Datentransfers ins EU-Ausland (Art. 57 Abs. 1 lit. r). Die Untersuchungs-, Abhilfe- (weiter als § 38 Abs. 5 BDSG) und Genehmigungsbefugnisse sind in Art. 58 DS-GVO geregelt, einer Norm, die gleich zwei Öffnungsklauseln für nationale Regelungen enthält. Gemäß Art. 58 Abs. 5 müssen die Mitgliedstaaten den nationalen Aufsichtsbehörden die Befugnis einräumen, „gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben". Art. 58 Abs. 6 erlaubt es darüber hinaus den Mitgliedstaaten, die Befugnisse der Aufsichtsbehörden zu erweitern.

Neu eingerichtet wird der Europäische Datenschutzausschuss, der die Art. 29-Datenschutzgruppe der DS-Richtlinie ersetzt und sich aus den Leitern der nationalen Aufsichtsbehörden zusammensetzt. Bei Mitgliedstaaten wie Deutschland, wo es mehrere Aufsichtsbehörden gibt, ist gemäß Art. 68 Abs. 4 DS-GVO ein gemeinsamer Vertreter zu bestimmen.[90] Der Europäische Datenschutzausschuss soll gemäß Art. 70 DS-GVO die einheitliche Anwendung der DS-GVO sicherstellen, hat dazu aber mit Stellungnahmen, Leitlinien und Empfehlungen vorwiegend nur beratende Kompetenzen, wie sich aus der langen Liste des Art. 70 Abs. 1 DS-GVO ergibt.[91]

Im Kommissionsentwurf von 2012 war noch das sog. One-Stop-Shop-Verfahren, also das Prinzip einer einheitlichen Anlaufstelle vorgesehen,[92] wonach die einzig zuständige Datenschutzbehörde für grenzüberschreitende datenschutzrechtliche Aktivitäten eines Unternehmens diejenige des Mitgliedstaates sein sollte, in dem das datenverarbeitende Unternehmen seine Hauptniederlassung hat. Das hätte dazu geführt, dass für Unternehmen mit Niederlassungen in mehreren Mitgliedstaaten nicht mehr unterschiedliche nationale Datenschutzbehörden zuständig gewesen wären. Da dieser Weg wenig bürgerfreundlich ist,[93] ist in der verabschiedeten DS-GVO dieser Ansatz zugunsten der von Datenverarbeitung Betroffenen abgeschwächt und durch das Kooperations- und Kohärenzverfahren in Art. 60 ff. DS-GVO ersetzt worden, bei dem Aufsichtsbehörden mehrerer Mitgliedstaaten zuständig sein können und der neu einzurichtende Europäische Datenschutzausschuss nach Art. 68 DS-GVO eine wichtige Rolle bei der einheitlichen Anwendung der DS-GVO spielen wird.[94]

Nur im Kohärenzverfahren, das der Berichterstatter des Europäischen Parlaments für den innovativsten Teil der Grundverordnung hält,[95] kann der vorwiegend beratend tätige Europäische Datenschutzausschuss nach Art. 65 in bestimmten, engen Fällen verbindliche Beschlüsse treffen. Das gilt grundsätzlich für alle Datenschutzfragen der DS-GVO, auch für den Beschäftigtendatenschutz. Es wird zunächst die federführende Aufsichtsbehörde i.S.v. Art. 56 DS-GVO bestimmt – sie richtet sich nach der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen in der EU. Die federführende Aufsichtsbehörde versucht gemäß

90 Vorschläge zur deutschen Vertretung im Europäischen Datenschutzausschuss bei *Kühling/Martini*, EuZW 2016, 448, 453.

91 *Roßnagel/Nebel/Richter*, ZD 2015, 455.

92 *Reding*, ZD 2012, 195, 196 f.

93 Daher war dieses Prinzip auch von der Konferenz der Datenschutzbeauftragten kritisiert worden: Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Struktur der künftigen Datenschutzaufsicht in Europa, 87. Konferenz der Datenschutzbeauftragten, 27.3.2014.

94 *Nguyen*, ZD 2015, 265.

95 *Albrecht*, CR 2016, 88, 96.

Art. 60 DS-GVO, mit den anderen betroffenen Aufsichtsbehörden einen Konsens zu erzielen. Wenn das nicht gelingt, tritt das Kohärenzverfahren nach Art. 63 ff. DS-GVO auf den Plan, in dem der Europäische Datenschutzausschuss in bestimmten Fällen nach Art. 65 verbindliche Beschlüsse erlassen kann. Die endgültige Entscheidung wird dann allerdings nach Einhaltung etlicher Fristen und weiterer Formalia von der nationalen Aufsichtsbehörde getroffen (Art. 65 Abs. 6 DS-GVO). Schließlich kann aber nach Art. 66 die nationale Aufsichtsbehörde „unter außergewöhnlichen Umständen" das Kohärenzverfahren überspielen und selbst einstweilige Maßnahmen treffen. Insgesamt dürfte das bürokratische Kohärenzverfahren eher zu einer Selbstlähmung der Aufsicht als in absehbarer Zeit zu einer Klärung der vielen offenen Auslegungsfragen und einem einheitlichen Gebrauch der Datenschutznormen der DS-GVO in den Mitgliedstaaten führen.

2. Rechtsschutz

Daher wird es besonders auf die Rolle der Rechtsprechung ankommen und zwar zum einen im Hinblick auf die Harmonisierungsfunktion des EuGH und zum anderen beim bereichsspezifischen Datenschutz, insbesondere beim Beschäftigtendatenschutz, auf die Rolle der nationalen (Arbeits-) Gerichte. Der einheitliche Rechtsrahmen der DS-GVO führt jedenfalls nicht zwingend zu einheitlicher Rechtsanwendung,[96] schon gar nicht, wenn es zahlreiche Öffnungen für mitgliedstaatliche Regelungen gibt.

a) Institutioneller Rechtsschutz

Neben einer Prozessvertretungsbefugnis i.S.v. Art. 80 Abs. 1 DS-GVO, die durch die Mitgliedstaaten gemäß Art. 80 Abs. 2 DS-GVO in ein Verbandsklagerecht erweitert werden kann,[97] sieht Art. 58 Abs. 5 DS-GVO vor, dass die Aufsichtsbehörden den Justizbehörden Datenschutzverstöße melden bzw. ggfs. gerichtliche Verfahren selbst einleiten oder sich daran beteiligen können. Die Mitgliedstaaten sind verpflichtet, die nähere Ausgestaltung in ihrem nationalen Recht vorzunehmen. Das Konzept ist nicht neu. Schon Art. 28 Abs. 3 DS-Richtlinie sieht Anzeige- und Klagerechte der Aufsichtsbehörde vor. In § 38 Abs. 1 S. 6 und § 44 Abs. 2 BDSG sind aber nur die Anzeigebefugnisse umgesetzt worden.

b) Individueller Rechtsschutz

Zunächst haben die nationalen (Arbeits-) Gerichte die DS-GVO wie auch alles andere EU-Recht anzuwenden und auszulegen. Wegen des Anwendungsvorrangs einer Verordnung gilt das auch, wenn das nationale Datenschutzrecht nicht außer Kraft gesetzt oder angepasst wird. Wenn sich vor den nationalen Gerichten Auslegungsfragen ergeben, die im Wege europarechtskonformer Auslegung nicht beantwortet werden können, kann bzw. wenn es sich um die letzte Instanz handelt, muss der EuGH nach Art. 267 AEUV im Wege der Vorabentscheidung angerufen werden, was Gerichtsverfahren deutlich verlängern wird, da die DS-GVO vor allem mit Generalklauseln arbeitet, die einen erheblichen Auslegungsbedarf nach sich ziehen werden. In Deutschland mit seinem umfassenden allgemeinen und bereichsspezifischen Datenschutzrecht gibt es bereits eine umfangreiche Rechtsprechung zum Datenschutz, die aber nicht ohne weiteres auf die Auslegung der DS-GVO übertragen werden kann. Es wird darauf

96 *Dieterich*, ZD 2016, 260.

97 Das Thema Verbandsklage wird im Zusammenhang mit den kollektiven Rechten im Beschäftigtendatenschutz behandelt, s.u. E.IV.2.

ankommen, was der deutsche Gesetzgeber im Einzelnen im Rahmen der Bereichsausnahmen der DS-GVO regelt. Ähnlich wie in der Rechtsvergleichung zwischen verschiedenen nationalen Rechtsordnungen, können gleiche oder ähnliche Begrifflichkeiten im nationalen und europäischen Recht nicht mit der Rechtsdogmatik eines Mitgliedstaates allein ausgelegt werden. Vielmehr ist die DS-GVO ein autonomer europäischer Rechtsakt, der vor dem Hintergrund seiner eigenen Entstehungsgeschichte sowie den Zielen und Zwecken, die der europäische Gesetzgeber ihm beigemessen hat, auszulegen ist.

Besonders brisant ist die Frage, inwieweit die Rechtsprechung des Bundesverfassungsgerichts zur informationellen Selbstbestimmung aus Art. 2 Abs. 1 und Art. 1 Abs. 1 GG ohne Einschränkung aufrechterhalten werden kann.[98] Grundsätzlich gilt, dass für Regelungen, die ihren Ursprung im EU-Recht haben, die GR-Charta der verfassungsrechtliche Maßstab ist. Haben sie ihren Ursprung im nationalen Recht, ist der Maßstab das GG.[99] Allerdings würden nationale Regelungen nicht losgelöst von der DS-GVO gelten, sondern auf ihrer Basis.

Darüber hinaus ist für den allgemeinen Datenschutz zu bedenken, dass Datenschutz auf der höheren, der europäischen, Ebene in Art. 8 GR-Charta speziell grundrechtlich geschützt ist. Das Verhältnis zwischen EU-Grundrechten und nationalen Grundrechten ist zwar nach wie vor nicht abschließend geklärt.[100] Für die DS-GVO und das deutsche Recht auf informationelle Selbstbestimmung ist aber zu berücksichtigen, dass die unmittelbar geltende Verordnung eine andere Perspektive einnimmt als das Recht auf informationelle Selbstbestimmung. Letzteres versteht den Datenschutz ausschließlich aus der Perspektive der betroffenen Person, also als Abwehrrecht, wie es für Grundrechte charakteristisch ist. In der DS-GVO hat der Datenschutz der betroffenen Person eher eine Abwägungsfunktion. Immer müssen auch die Interessen des Datenverwenders berücksichtigt werden. Schon im ersten Artikel der DS-GVO wird deutlich, dass der freie Verkehr personenbezogener Daten gleichgewichtig neben dem Datenschutz steht. Das ist für sich betrachtet auch konsequent, da es sich bei der DS-GVO nicht primär um eine verfassungsrechtliche Schutzregelung, sondern um eine Binnenmarktregelung handelt. Da jedenfalls die Grundprinzipien der DS-GVO durch mitgliedstaatliche Gesetzgebung nicht ausgehebelt werden dürfen, hat die Rechtsprechung des BVerfG zur informationellen Selbstbestimmung für das in der DS-GVO geregelte allgemeine Datenschutzrecht nur insoweit Bestand als diesem Perspektivenwechsel im Datenschutz Rechnung getragen wird.

In Zukunft fällt der verfassungsrechtliche Schutz des Betroffenen in den Bereichen, für die die DS-GVO keine mitgliedstaatliche Öffnung enthält, dem EuGH zu. In diesen Fällen steht der Individualrechtsbehelf Verfassungsbeschwerde dann nicht mehr zur Verfügung. Der EuGH hat sich in der jüngsten Vergangenheit mehrfach mit Datenschutzfragen befasst und in drei wichtigen Urteilen – der Ungültigerklärung der EU-Richtlinie zur Vorratsdatenspeicherung,[101] zu Google[102] und zu Facebook[103] – persönlichkeitsschutzfreundliche Lösungen gefunden. In diesen Fällen war die zunächst geäußerte Befürchtung unbegründet, dass der EuGH als für sämtliche mit dem Binnenmarkt zusammenhängenden Fragen allzuständiges Gericht, auf die in Deutschland besonders starke verfassungsrechtliche Seite des Datenschutzes nicht vorberei-

98 Zu den verfassungsrechtlichen Problemen, insbesondere dem Verhältnis von BVerfG und EuGH schon *Körner*, Die Reform des EU-Datenschutzes: Der Entwurf einer EU-Datenschutz-Grundverordnung (DS-GVO), Teil II, ZESAR 2013, 153, 155 ff.; grundlegend dazu: *Pötters, Stephan*, Grundrechte und Beschäftigtendatenschutz, 2013.

99 *Heuschmid*/Lörcher, NK-GA, Art. 51 Rn. 23-26; BVerfG, Urt. v. 15.12.2015 – 2 BvR 2735/14. Im Übrigen siehe schon oben C.I.2 und 3.

100 Dazu schon oben C.I.3.

101 EuGH, Urt. v. 8.4.2014 – C-293/12, C-594/12, DuD 2014, 488.

102 EuGH, Urt. v. 13.5.2014 – C-131/12, DuD 2014, 559.

103 EuGH, Urt. v. 6.10.2015 – C-362/14, DuD 2015, 823.

tet und daher das bisherige, durch das BVerfG gewährte hohe Schutzniveau in Zukunft nicht zu gewährleisten sei.

Allerdings handelt es sich nur um wenige Fälle, in denen der EuGH sich zu Datenschutzfragen äußern konnte. Das europäische Gericht hatte bislang viel zu selten Gelegenheit, sich mit dem Grundrecht auf Datenschutz aus Art. 8 GR-Charta zu befassen (und konnte es daher nicht effizient schützen).

In Zukunft wird also die Interpretation der unbestimmten Rechtsbegriffe der DS-GVO zunächst den einzelstaatlichen Gerichten obliegen, die sich einerseits an den bisherigen unterschiedlichen Datenschutzkulturen in den Mitgliedstaaten orientieren werden und die andererseits nicht an die Auslegungsergebnisse der Aufsichtsbehörden gebunden sind, denn diese sind, auch nach einem Kohärenzverfahren, nur an die beteiligten Aufsichtsbehörden adressiert und haben keine allgemeine Rechtswirkung. Selbst national gibt es nur Rechtsklarheit, wenn oberste Gerichte in einzelnen Fällen entscheiden. Europäisch gilt das erst recht: nur in Einzelfällen – mögen Sie auch typisch sein – kann der EuGH in einem jahre- bis jahrzehntelangen Prozess Einzelfragen beantworten. Der Rechtssicherheit sowohl für Datenverarbeiter wie für Betroffene ist das abträglich.[104]

VIII. Übermittlung an Drittstaaten

Die in Art. 44 ff. DS-GVO geregelte Datenübermittlung in Drittstaaten entsprechen im Wesentlichen dem geltenden Recht. Es bleibt gemäß Art. 45 Abs. 3 bei der Adäquanzentscheidung der Kommission, der Datenübermittlungsmöglichkeit aufgrund geeigneter Datenschutzgarantien gemäß Art. 46 oder von der Aufsichtsbehörde genehmigter Binding Corporate Rules nach Art. 47. Als Garantie i.S.v. Art. 46 gelten nun auch von der Kommission im Wege delegierter Rechtsakte für allgemeinverbindlich erklärte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m. Art. 40 Abs. 9) und zertifizierte Datenschutzregeln (Art. 46 Abs. 2 lit. f i.V.m. Art. 42). Liegen die genannten Voraussetzungen nicht vor, erlaubt Art. 49 Abs. 1 lit. a - g Ausnahmen für bestimmte Fälle, wie das Erfordernis der Datenübermittlung für die Erfüllung eines Vertrages. Als ganz besondere Ausnahme wird dann in Art. 49 S. 2 i.V.m. Erwägungsgrund 113 noch der Fall angefügt, dass der Verantwortliche „zwingende berechtigte Interessen“ geltend machen kann. Dann muss zumindest die Aufsichtsbehörde im Nachhinein von der Übermittlung in Kenntnis gesetzt und der Betroffene informiert werden.

Das auf die Beharrlichkeit eines österreichischen Jurastudenten zurückgehende Safe Harbor-Urteil des EuGH[105] untersagt dem US-amerikanischen Unternehmen Facebook den Transfer personenbezogener Daten von EU-Bürgern in die USA, solange dort keine ausreichenden Datenschutzregeln gelten. Damit hat der EuGH die von der Kommission seit dem Jahr 2000 geübte Praxis des Datentransfers von der EU in die USA gegen im Prinzip nicht mehr als das Versprechen des Empfängers, Datenschutz zu gewähren,[106] ohne Einschränkungen verboten. Dennoch bleibt der Datentransfer aus der EU in Drittstaaten auch in Zukunft die Achillesferse des europäischen Datenschutzes, da die neuen von der Kommission mit den USA ausgehandelten Privacy Shield-Regeln noch weit von Art. 8 GR-Charta entfernt sind.[107]

104 *Roßnagel*, Schriftliche Stellungnahme zum öffentlichen Fachgespräch zur Datenschutz-Grundverordnung am 24. Februar 2016 im Ausschuss Digitale Agenda des Deutschen Bundestages, S. 15.

105 EuGH, Urt. v. 6.10.2015 – C-362/14, NJW 2015, 3151.

106 KOM 2000/520/EG (Safe Harbor).

107 *Weichert*, ZD 2016, 209, 217; vgl. auch die ausführliche Darstellung mit vergleichbarer Skepsis, was die Position des EuGH angeht: *Grau/Granetzny*, NZA 2016, 405.

Zwar haben die Aufsichtsbehörden nun gemäß Art. 58 Abs. 2 lit. j DS-GVO die Befugnis, die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland anzuordnen. Die Reichweite dieses Rechtes ist aber dennoch umstritten.[108] In der Safe Harbor-Entscheidung – die sich aber auf Art. 28 Abs. 3 der DS-Richtlinie bezieht – hat der EuGH zwar einerseits festgestellt, dass die Befugnisse der Aufsichtsbehörden nicht durch die Entscheidungskompetenz der Kommission für Drittstaatenübermittlungen beschnitten werden dürfen.[109] Andererseits hat der EuGH aber klargestellt, dass nur er selbst eine derartige Entscheidung der Kommission nach Art. 25 Abs. 6 DS-Richtlinie aufheben darf.[110] Obwohl das auch schon in den nicht abschließend formulierten Art. 28 Abs. 3 DS-Richtlinie hineingelesen wurde,[111] hat der EuGH diese Vorstellung nicht in die Safe Harbor-Entscheidung übernommen. Der Umgang des EuGH mit der Privacy Shield-Vereinbarung angesichts des neuen Art. Art. 58 Abs. 2 lit. j DS-GVO, wenn er denn Gelegenheit bekommt, sie zu bewerten, bleibt abzuwarten.[112] Jedenfalls wird die Privacy-Shield-Vereinbarung den Grundsätzen des Safe-Harbor-Urteils entsprechen müssen, wonach eine Angemessenheit des Datenschutzniveaus der USA nur in Betracht kommt, wenn die Zugriffsbefugnisse der US-Sicherheitsbehörden auf das „absolut Notwendige“ beschränkt sind und europäische Bürger die Möglichkeit haben, bei einem Gericht einen wirksamen Rechtsbehelf einzulegen.[113] Klar hat der EuGH festgestellt, dass eine Regelung nicht auf das absolut Notwendige beschränkt ist, „die generell die Speicherung aller personenbezogenen Daten sämtlicher Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt wurden, gestattet, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels vorzunehmen und ohne ein objektives Kriterium vorzusehen, das es ermöglicht, den Zugang der Behörden zu den Daten und deren spätere Nutzung auf ganz bestimmte, strikt begrenzte Zwecke zu beschränken, die den sowohl mit dem Zugang zu diesen Daten als auch mit deren Nutzung verbundenen Eingriff zu rechtfertigen mögen“.[114]

Eine weitere Einschränkung deutet sich an: In seinem Schlussantrag vom 8. September 2016 hat der Generalanwalt beim Europäischen Gerichtshof Paolo Mengozzi aufgrund eines Gutachtenauftrags des Europäischen Parlaments das Abkommen zwischen der EU und Kanada zur Fluggastdatenverarbeitung in mehreren Punkten für unvereinbar mit der GR-Charta gehalten.[115] Diese Rechtsansicht dürfte auch Auswirkungen auf die entsprechenden Abkommen mit den USA und Australien sowie auf den Umgang mit der im April 2016 beschlossenen EU-Richtlinie über die Verwendung von Fluggastdaten haben.

IX. Fazit: Fortschritte und Defizite der DS-GVO

Die DS-GVO wird nicht ganz zu Unrecht z.T. für unterkomplex gehalten,[116] da sie kaum normative Inhalte hat, auch wenn es vor allem zum Verfahren Verbesserungen gibt, wie Art. 35

108 Vgl. *Dieterich*, ZD 2016, 260, 263 m.w.N.
109 EuGH, Urt. v. 6.10.2015, C-362/14, NJW 2015, 3151, Rn. 53.
110 A.a.O., Rn. 61.
111 EuGH, Schlussantrag v. 23.9.2015 – C-362/14,BeckRS 2015, 81603, Rn. 94; so auch in der Lit.: *Bergt*, Anm. zu EuGH (Safe Harbor), MMR 2015, 753; *Kühling/Heberlein*, NvWZ 2016, 7, 8.
112 Zweifelnd *Dieterich*, ZD 2016, 260, 264.
113 So auch *Roßnagel,* Stellungnahmen zum öffentlichen Fachgespräch zur Datenschutz-Grundverordnung, 24.2.2016, Ausschuss Digitale Agenda des Deutschen Bundestages, S. 13.
114 EuGH, Urt. v. 6.10.2015 – C-362/14, NJW 2015, 3151, Rn. 83.
115 Schlussanträge des Generalanwalts Paolo Mengozzi vom 8. September 2016, Gutachten 1/15, http://curia.europa.eu/juris/document/document_print.jsf;jsessionid=9.
116 Begriff *Roßnagel/Nebel/Richter*, ZD 2015, 455, 460.

zur Folgenabschätzung, Art. 12–15 zur Transparenz oder Art. 85 Abs. 2, dem der bisherige § 41 BDSG zur Freistellung der Presse von Datenschutzvorgaben nicht entspricht.[117]

Die beschworene Technikneutralität ist allerdings ein Mythos.[118] Wenn damit gemeint sein sollte, dass die Regelungen der DS-GVO auch für zukünftige digitale Technik ausreichend Schutz gewähren sollte, so wäre dieser Anspruch vermessen, da allenfalls absehbar ist, dass sich die digitale Technik weiterhin in hohem Tempo entwickeln wird, nicht aber, welche weiteren (Kontroll-) Möglichkeiten sich daraus in Zukunft ergeben und welche Regelungen dann nötig sein werden. Insofern hat man es in diesem Bereich immer mit einem „offenen Regelungsprozess“[119] zu tun. Wahrscheinlich ist Technikneutralität laut Erwägungsgrund 15 viel bescheidener gemeint, insofern es für den Schutz personenbezogener Daten nicht auf den Umstand ankommen soll, ob sie automatisiert oder manuell verarbeitet werden.

Zentrale Datenschutzprobleme bei Big Data, Smart Data oder Cloud Computing werden nicht gelöst, aber das könnte gerade gewollt sein, da es sich bei den genannten Formen von Datennutzung um wirtschaftliche Zukunftsmodelle handelt. Für das Cloud Computing ist Art. 28 Abs. 5 DS-GVO denn auch eher eine Erleichterung als eine Datenschutzvorschrift mit Fokus auf dem Persönlichkeitsrecht. Nach Art. 28 Abs. 4 haftet der Verantwortliche zwar für Datenschutzverstöße durch Auftragnehmer. Nach Art. 28 Abs. 5 reicht es aber als Datenschutzgarantie i.S.v. Art. 28 Abs. 1 aus, wenn der Auftragnehmer die Einhaltung genehmigter Verhaltensregeln (nach Art. 40) oder eines zertifizierten Verfahrens zusagt.

Die DS-GVO geht noch ausschließlich vom althergebrachten Rechenzentrumskonzept der ersten Datenschutzregelungen aus, d.h. von einer verantwortlichen Stelle, die in der EU „greifbar“ ist und bestimmte Regeln einhalten muss, was auch kontrolliert werden kann. Neue Konzepte für den Datenschutz im Internet enthält die Verordnung nicht, z.B. ein schon länger gefordertes eingebautes Verfallsdatum für gespeicherte Daten[120] oder/und den sog. digitalen Radiergummi.[121] Datenschutz durch Technik[122] wird nur unspezifisch angesprochen, aber nicht (auf dem heutigen Stand der Technik) wenigstens in den Erwägungsgründen näher konturiert. So bleibt es den Anwendern überlassen, ob und was sie an technischem Datenschutz einführen wollen.

Auch die Datenschutzprinzipien, auf denen die Verordnung basiert, stammen aus den Anfangszeiten des Datenschutzes vor 45 Jahren.[123] Gerade dieser Umstand mag zu einer gewissen Beruhigung der vier Jahre lang aufgeregten Diskussion um – je nach Perspektive – zu viel oder zu wenig Datenschutz auf EU-Ebene geführt haben, denn die Prinzipien sind die vertrauten, allen voran der Zweckbindungsgrundsatz. Vor dem Hintergrund von Big Data allerdings, einer Datenauswertungsmethode, bei der es sich nicht um eine von vielen Verfahren, sondern um einen zentralen, längst global eingesetzten Mechanismus handelt, der in Zukunft jede Art von komplexer Organisationsplanung, Versorgungs- und Investitionsentscheidung, kurz alle Arten von Prognosen prägen wird, läuft der Zweckbindungsgrundsatz schon heute leer. Für Big Data-Anwendungen besteht der Wert der personenbezogenen Information gerade nicht im ursprünglichen Zweck, sondern in der Wiederverwertung einmal gesammelter Daten zu ganz anderen, im Zeitpunkt der Erhebung oft noch gar nicht bekannten Zwecken. Hier jeweils die

117 Auch schon Art. 9 der DS-Richtlinie hatte § 41 BDSG nicht entsprochen: Simitis-*Dix*, BDSG-Kommentar, 8. Auflg., § 41 Rn. 2.

118 *Sydow/Kring*, ZD 2014, 271; Zu Datenschutz durch Technik siehe unten E.II.4.

119 *Simitis*, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 8. Auflg., Einleitung, Rn. 106.

120 *Simitis*, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 8. Auflg., Einleitung Rn. 122.

121 Dazu umfassend: *Mayer-Schönberger*, Delete, 2010, 199 ff.

122 Dazu *Maas/Schmitz/Wedde*, Datenschutz 2014 – Probleme und Lösungsmöglichkeiten, Frankfurt 2014. Zu diesem wichtigen Konzept siehe noch unten E.II.4.

123 Das Fehlen innovativer Lösungsansätze bemängelt auch *Härting/Schneider*, CR 2015, 819.

erneute Zustimmung aller Betroffenen zur Zweckänderung zu verlangen, geht an der digitalen Realität vorbei. Google dürfte sich kaum mit Hunderten Millionen Nutzern seiner Suchmaschine in Verbindung setzen, um die Zustimmung zur Verwendung alter Suchanfragen für die Vorhersage einer Grippewelle einzuholen, auch wenn das technisch möglich wäre.[124] Das Phänomen wird seit mindestens zehn Jahren beschrieben,[125] hat aber in die Verhandlungen um die DS-GVO und vor allem in deren Ergebnis kaum Eingang gefunden. Allerdings enthält die Verordnung etwas versteckt mit Art. 6 Abs. 4 eine Norm, die unter bestimmten Voraussetzungen spätere Zweckänderungen erlaubt und daher durchaus als Rechtsgrundlage herangezogen werden könnte, ohne den Schutzaspekt ausreichend zu thematisieren. Hier fehlen neue datenschutzrechtliche Modelle.[126]

Angesichts der beiden möglichen Regelungsmodelle – bereichsspezifisch-kasuistisch versus generell-abstrakt, die jeweils in ihrer Reinform Nachteile mit sich bringen – hat sich der europäische Gesetzgeber für eine vorwiegend generalklauselartige Regulierung entschieden. Anders wäre es auch kaum möglich, in 99 Artikeln das gesamte Datenschutzrecht im öffentlichen und nicht-öffentlichen Bereich abzudecken. Auch wenn in einem von rasanter technischer Entwicklung geprägten Rechtsgebiet eine vorwiegend kasuistische Regelung wegen ihrer Unübersichtlichkeit, aber auch weil sie schnell veraltet, jedenfalls für den allgemeinen Datenschutz – im bereichsspezifischen Datenschutz kann es anders aussehen – nicht empfehlenswert ist, führt der nun gewählte Weg mit vielen inhaltsleeren und nahezu beliebig füllbaren Kriterien zu großer Rechtsunsicherheit, was etwa die Interessenabwägungsklausel in Art. 6 Abs. 1 lit. f DS-GVO belegt.[127]

Diese sehr vagen allgemeinen Regelungen sprechen ganz besonders dafür, dass die Mitgliedstaaten gehalten sind, von den zahlreichen nationalen Regelungsbefugnissen Gebrauch zu machen, die die DS-GVO (fast schon wie eine Richtlinie) bietet. Das gilt auch und gerade für die fakultativen nationalen Regelungsbefugnisse, weil ansonsten „eine nicht hinnehmbare Rechtsunsicherheit“ entstünde.[128]

Die Fortschritte der DS-GVO liegen auf der Verfahrensebene, die für die tatsächliche Durchsetzung der materiellrechtlichen Ansprüche zentral ist. Die entscheidende Neuerung ist die Einführung des Marktortprinzips, wonach die DS-GVO auf die Verarbeitung aller personenbezogenen Daten innerhalb der EU anwendbar ist, unabhängig davon, wo der Datenverarbeiter seinen Sitz hat. Darüber hinaus stellt es für den Datenschutz in den meisten Mitgliedstaaten einen großen Fortschritt dar, dass nun in allen Mitgliedstaaten unabhängige Datenschutzbehörden geschaffen werden müssen, die für die Überwachung der Einhaltung der DS-GVO in ihrem jeweiligen Land zuständig sind. Wichtig ist auch der Koordinationsmechanismus durch den Europäischen Datenschutzausschuss, der die einheitliche Anwendung der DS-GVO-Regeln in allen Mitgliedstaaten garantieren soll, wenn hier auch abzuwarten bleibt, als wie effizient sich das Verfahren in der Praxis erweisen wird. Schließlich stehen die Sanktionsregelungen auf der Haben-Seite der Verordnung, insbesondere die hohen Bußgelder. Auch hier wird aber erst die Zukunft zeigen, inwieweit diese in der Praxis tatsächlich verhängt werden.

124 Beispiel aus *Mayer-Schönberger/Cukier*, Big Data, 2013, 2. Auflg., S. 193.

125 U.a. *Cate, Fred*, The Failure of Fair Information Practice Principles, in: Winn, Jane (Hrsg.), Consumer Protection in the Age of the “Information Economy”, Ashgate 2006, S. 341 ff.

126 So auch *Dammann*, ZD 2016, 307, 313.

127 So auch *Buchner*, DuD 2016, 155, 159; *Sydow/Kring*, ZD 2014, 271, 272.

128 *Kühling/Martini*, EuZW 2016, 448, 449.

Literaturverzeichnis

Albrecht, Jan Philipp, Die EU-Datenschutzgrundverordnung rettet die informationelle Selbstbestimmung! Ein Zwischenruf für einen einheitlichen Datenschutz durch die EU, ZD 2013, 587 – 590.

- Das neue EU-Datenschutzrecht, CR 2016, 88 – 98.

Ashkar, Daniel, Durchsetzung und Sanktionierung des Datenschutzrechts nach den Entwürfen der Datenschutz-Grundverordnung, DuD 2015, 796 – 800.

Bergt, Matthias, Anm. zu EuGH (Safe Harbor), MMR 2015, 753 – 762.

Boeken, Winfried/Düwell, Franz Josef/Diller, Martin/Hanau, Hans (Hrsg.), Gesamtes Arbeitsrecht, 2016 (NomosKommentar: NK-GA).

Buchner, Benedikt, Informationelle Selbstbestimmung im Privatrecht, Tübingen, 2006.

- Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, DuD 2016, 155 – 161.

Bundesministerium für Arbeit und Soziales (Hrsg.), Grünbuch – Arbeiten 4.0, Berlin, 2015.

Cate, Fred, The Failure of Fair Information Practice Principals, in: Winn, Jane (Hrsg.), Consumer Protection in the Age of the "Information Economy", Ashgate, 2006.

Dammann, Ulrich, Erfolge und Defizite der EU-Datenschutzgrundverordnung, ZD 2016, 307 – 314.

Däubler, Wolfgang, Internet und Arbeitnehmerdatenschutz, AiB extra 2015, 29 – 32.

- Digitalisierung und Arbeitsrecht, SR Sonderausgabe Juli 2016.

Dederer, Hans-Georg, Die Grenzen des Vorrangs des Unionsrechts – Zur Vereinheitlichung von Grundrechts-, Ultra-vires- und Identitätskontrolle, JZ 2014, 313.

Dieterich, Thomas, Rechtsdurchsetzungsmöglichkeiten der DS-GVO, ZD 2016, 260 – 266.

Dix, Alexander, Datenschutzaufsicht im Bundesstaat – ein Vorbild für Europa, DuD 2012, 318 – 321.

Faust, Sebastian/Spittka, Jan/Wybitul, Tim, Milliardenbußgelder nach der DS-GVO? Ein Überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz, ZD 2016, 120 – 125.

Franck, Lorenz, System der Betroffenenrechte nach der Datenschutz-Grundverordnung (DS-GVO), RDV 2016, 111 – 119.

Gierschmann, Sibylle, Was bringt deutschen Unternehmen die DS-GVO? Mehr Pflichten, aber die Rechtsunsicherheit bleibt, ZD 2016, 51 – 55.

Giesen, Richard/Junker, Abbo/Rieble, Volker, Industrie 4.0 als Herausforderung des Arbeitsrechts, ZAAR Schriftenreihe, Band 39, München, 2016.

Gola, Peter/Schomerus, Rudolf, Bundesdatenschutzgesetz. BDSG, Kommentar, 12. Aufl., München, 2015.

Gola, Peter/Schulz, Sebastian, Der Entwurf für eine EU-Datenschutz-Grundverordnung - eine Zwischenbilanz, RDV 2013, 1 – 7.

Grau, Timon/Grantzny, Thomas, EU-US-Privacy Shield - Wie sieht die Zukunft des transatlantischen Datenverkehrs aus?, NZA 2016, 405 – 410.

Grimm, Dieter, Der Datenschutz vor einer Neuorientierung, JZ 2013, 585 – 592.

Härting, Niko/Schneider, Jochen, Das Ende des Datenschutzes - es lebe die Privatsphäre, CR 2015, 819 – 827.

Hornung, Gerrit, Eine Datenschutz-Grundverordnung für Europa? Licht und Schatten im Kommissionsentwurf vom 25.1.2012, ZD 2012, 99 – 106.

Keppeler, Lutz, Was bleibt vom TMG-Datenschutz nach der DS-GVO? Lösung und Schaffung von Abgrenzungsproblemen im Multimedia-Datenschutz, MMR 2015, 779.

Kingreen, Thorsten, Die Grundrechte des Grundgesetzes im europäischen Grundrechtsföderalismus, JZ 2013, 801 – 811.

Kingreen, Thorsten/Kühling, Jürgen, Weniger Schutz durch mehr Recht: Der überspannte Parlamentsvorbehalt im Datenschutzrecht – Eine Problemskizze am Beispiel des Gesundheitsdatenschutzrechts –, JZ 2015, 213 – 221.

Körner, Marita, Informierte Einwilligung als Schutzkonzept, in: Simon, Dieter/Weiss, Manfred (Hrsg.), Zur Autonomie des Individuums, Liber Amicorum Spiros Simitis, Baden-Baden, 2000, S. 131 – 150.

- Regierungsentwurf zum Arbeitnehmerdatenschutz, AuR 2010, 416 – 421.

- Die Reform des EU-Datenschutzes - Der Entwurf einer EU-Datenschutz-Grundverordnung (DS-GVO) - Teil I, ZESAR 2013, 99 – 107.

- Die Reform des EU-Datenschutzes - Der Entwurf einer EU-Datenschutz-Grundverordnung (DS-GVO) - Teil II, ZESAR 2013, 153 – 159.

Kort, Michael, Arbeitnehmerdatenschutz gemäß der EU-Datenschutz-Grundverordnung, DB 2016, 711 – 716.

Kraska, Sebastian, Auswirkungen der EU-Datenschutzgrundverordnung, ZD-Aktuell 2016, 04173.

Krause, Rüdiger, Verhandlungen des 71. Deutschen Juristentages, Band I: Gutachten / Teil B: Digitalisierung der Arbeitswelt - Herausforderungen und Regelungsbedarf, Essen, 2016.

Kühling, Jürgen, Rückkehr des Rechts: Verpflichtung von „Google & Co." zu Datenschutz, EuZW 2014, 527 – 532.

Kühling, Jürgen/Heberlein, Johanna, EuGH „reloaded": „unsafe harbor" USA vs. „Datenfestung" EU, NVwZ 2016, 7 – 12.

Kühling, Jürgen/Martini, Mario, Die Datenschutzgrundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, 448 – 454.

Kühling, Jürgen/Martini, Mario/Heberlein, Johanna/Kühl, Benjamin/Nink, David/Weinzierl, Quirin/Wenzel, Michael, Die Datenschutz-Grundverordnung und das nationale Recht, Erste Überlegungen zum innerstaatlichen Regelungsbedarf, Münster, 2016.

Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios, Datenschutzrecht, Kommentar, 3. Aufl., Heidelberg, 2015.

Maas, Heiko, EU-Datenschutz-Grundverordnung: Datensouveränität in der digitalen Gesellschaft, DuD 2015, 579 – 580.

Maas, Ingrid/Schmitz, Karl/Wedde, Peter, Datenschutz 2014 – Probleme und Lösungsmöglichkeiten, Frankfurt a.M., 2014.

Masing, Johannes, Einheit und Vielfalt des Europäischen Grundrechtsschutzes, JZ 2015, 477 – 487.

Mayer-Schönberger, Viktor, Delete – Die Tugend des Vergessens in digitalen Zeiten, 3. Aufl., Wiesbaden, 2015.

Mayer-Schönberger, Viktor/Cukier, Kenneth, Big Data – Die Revolution die unser Leben verändern wird, 2. Aufl., München, 2013.

Nguyen, Alexander, Die zukünftige Datenschutzaufsicht in Europa, ZD 2015, 265 – 270.

Pötters, Stephan, Grundrechte und Beschäftigtendatenschutz, Baden-Baden, 2013.

Polzin, Monika, Das Rangverhältnis von Verfassungs- und Unionsrecht nach der neuesten Rechtsprechung des BVerfG, JuS 2012, 1 – 6.

Reding, Viviane, Sieben Grundbausteine der europäischen Datenschutzreform, ZD 2012, 195 – 198.

Richter, Philipp, Datenschutz zwecklos? – Das Prinzip der Zweckbindung im Ratsentwurf der DSGVO, DuD 2015, 735 – 740.

Rossnagel, Alexander, Datenschutz in einem informatisierten Alltag, Gutachten im Auftrag der Friedrich-Ebert-Stiftung, Berlin, 2007.

- Schriftliche Stellungnahme zum öffentlichen Fachgespräch zur Datenschutz-Grundverordnung am 24. Februar 2016 im Ausschuss Digitale Agenda des Deutschen Bundestags, 24.02.2016.

Rossnagel, Alexander/Kroschwald, Steffen, Was wird aus der Datenschutzgrundverordnung? Die Entschließung des Europäischen Parlaments über ein Verhandlungsdokument, ZD 2014, 495 – 500.

Rossnagel, Alexander/Nebel, Maxi/Richter, Philipp, Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO, ZD 2015, 455 – 460.

Schantz, Peter, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, 1841 – 1847.

Schild, Hans-Hermann/Tinnefeld, Marie-Theres, Datenschutz in der Union – Gelungene oder missglückte Gesetzentwürfe?, DuD 2012, 312 – 317.

Simitis, Spiros, Die EG-Datenschutzrichtlinie: eine überfällige Reformaufgabe, in: Herzog, Felix/ Neumann, Ulfried (Hrsg.), Festschrift für Winfried Hassemer, Heidelberg, 2010, S. 1235 – 1248.

- Bundesdatenschutzgesetz, 8. Aufl., Baden-Baden, 2014.

Sydow, Gernot/Kring, Markus, Die Datenschutzgrundverordnung zwischen Technikneutralität und Technikbezug, ZD 2014, 271 – 276.

Wedde, Peter, Die unterschätzte Macht der Mitbestimmung, CuA 2016, 8 – 13.

Weichert, Thilo, EU-US-Privacy Shield - ist der transatlantische Datentransfer nun grundrechtskonform?, ZD 2016, 209 – 217.

Rechtswissenschaftliche Beiträge der Hamburger Sozialökonomie

ISSN 2366-0260 (print)
ISSN 2365-4112 (online)

Bislang erschienene Hefte:

Heft 1
Felix Boor, Die Yukos-Enteignung. Auswirkungen auf das Anerkennungs- und Vollstreckungssystem aufgehobener ausländischer Handelsschiedssprüche

Heft 2
Karsten Nowrot, Sozialökonomie als disziplinäre Wissenschaft.
Alternative Gedanken zur sozialökonomischen Forschung, Lehre und (Eliten-) Bildung

Heft 3
Florian Hipp, Die kommerzielle Verwendung von frei zugänglichen Inhalten im Internet

Heft 4
Karsten Nowrot, Vom steten Streben nach einer immer wieder neuen Weltwirtschaftsordnung.
Die deutsche Sozialdemokratie und die Entwicklung des Internationalen Wirtschaftsrechts

Heft 5
Karsten Nowrot, Jenseits eines abwehrrechtlichen Ausnahmecharakters. Zur multidimensionalen Rechtswirkung des Widerstandsrechts nach Art. 20 Abs. 4 GG

Heft 6
Karsten Nowrot, Grundstrukturen eines Beratungsverwaltungsrechts

Heft 7
Karsten Nowrot, Environmental Governance as a Subject of Dispute Settlement Mechanisms in Regional Trade Agreements

Heft 8
Margaret Thornton, The Flexible Cyborg: Work-Life Balance in Legal Practice

Heft 9
Antonia Fandrich, Sustainability and Investment Protection Law. A Study on the Meaning of the Term *Investment* within the ICSID Convention

Heft 10
Karsten Nowrot, Of "Plain" Analytical Approaches and "Savior" Perspectives: Measuring the Structural Dialogues between Bilateral Investment Treaties and Investment Chapters in Mega-Regionals

Heft 11
Maryna Rabinovych, The EU Response to the Ukrainian Crisis: Testing the Union's Comprehensive Approach to Peacebuilding